华章数学译丛

32

# A Course in Combinatorics (Second Edition)

# 组合数学教程

（原书第2版）

（荷）J. H. van Lint
（美）R. M. Wilson 著
刘振宏 赵振江 译

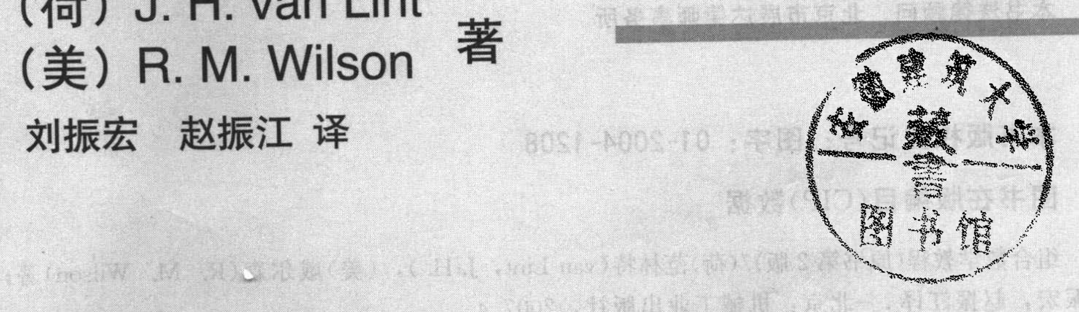


华章数学译丛

32



# A Course in Combinatorics (Second Edition)



(原书第2版)

(荷) J. H. van Lint
(美) R. M. Wilson 著
刘振宏 赵振江 译



机械工业出版社
China Machine Press

（原书第2版）

# 组合数学教程

本书是一本在国际上受到学者推崇的组合数学教科书，被美国哥伦比亚大学、斯坦福大学、加州理工学院等众多著名大学采纳为教材。

本书讲述的内容非常广泛，讨论的问题涵盖组合数学所涉及的绝大部分领域，堪称“组合数学的百科全书”。本书不仅包含了一般组合数学教科书中的经典内容，而且收集了若干新的内容，如Lovász筛法、范德瓦尔登积和式猜想、结合区组设计、码和设计等。作者的阐述深入浅出，使得高深的内容简明易懂，便于广大读者阅读。

## 作 者 简 介



**J. H. van Lint (1932－2004)** 拥有荷兰乌特勒支大学博士学位，是荷兰埃因霍温科技大学数学与计算机科学系教授，于1997年退休。他是荷兰皇家艺术和科学院成员、西安交通大学荣誉教授、荷兰数学会荣誉成员等。除本书外，他还著有《Introduction to Coding Theory》、《Coding Theory》等书。



**R. M. Wilson** 在俄亥俄州立大学上学期间，他与D. K. Ray-Chaudhuri一起解决了Kirkman女生问题。1969年，他于俄亥俄州立大学获得博士学位，并任教于该校。1975年，他因设计的渐近存在方面的工作而获得SIAM（美国工业和应用数学学会）组合数学方面的George Polya奖。1980年，他成为加州理工学院数学教授。他的研究兴趣包括组合设计理论、极集理论、编码论中的代数问题和组合问题等。

**A Course in Combinatorics**
(Second Edition)





影印版
ISBN 7-111-13992-5
定价：58.00 元





封面设计·杨宇梅




华章图书


华章网站 http://www.hzbook.com
网上购书：www.china-pub.com
投稿热线：(010) 88379604
购书热线：(010) 68995259, 68995264
读者信箱：hzjsj@hzbook.com





ISBN 978-7-111-20595-1
定价：49.00 元

# 译 者 序

组合数学是计算机出现以后迅速发展起来的一个数学分支，它不仅在基础数学研究中占据极其重要的地位，而且在计算机科学、编码和密码学、物理、化学、生物等学科中也有重要的应用.

本书译自 J. H. van Lint 和 R. M. Wilson 所著的《A Course in Combinatorics，Second Edition》一书，这是一本在国际上受到学者推崇的组合数学教科书，其特点如下：

1. 内容非常广泛：全书共 38 章，是目前我们所见到的国内外组合数学教程中最为全面的一本，几乎涵盖了组合数学的所有领域. 正如作者在前言中所说的那样，读完此书的读者在参加组合数学会议时，不会因为对某个专题不熟悉而完全听不懂别人的报告，他至少能听到一些熟悉的词语，知道报告人在说什么.

2. 材料丰富新颖：本书不仅包含了一般组合数学教科书中的经典内容，而且收集了若干新的内容. 例如，Lovász 筛法、范德瓦尔登积和式猜想、结合区组设计、码和设计、图的目录染色等，其中有的内容鲜为人知，有些例子饶有趣味.

3. 材料编排与众不同：与数学的其他学科不同，组合数学迄今还没有一套完整的理论体系，组合数学中的专题(或分支)之间的独立性很大. 因此，在组合数学的教科书中，几乎都是按专题划分章节. 但本书不完全依此惯例，而是将某些专题分拆插入其他专题，比如偏序集和码，特别是计数和图论专题更是遍及全书.

本书涉及的基础理论虽然比较广泛，如代数，特别是抽象代数；几何，特别是投影几何；数学分析和初等数论等，但只需掌握其基本概念以及会灵活运用即可.

从本书的深度和广度来看，本书可以作为高等院校相关专业高年级本科生和低年级研究生的组合数学课程教材或教学参考书，同时也可以作为从事组合数学教学和研究的人员的参考书.

由于译者水平所限，译文中难免出现错误和不妥之处，恳请读者不吝赐教.

译　者

于北京

# 第1版前言

H. J. Ryser 在加州理工学院讲授的“数学 121”课程“组合分析”，是最受欢迎的高水平的数学课程之一，这一课程开设了许多年. Ryser 的主要目标之一是说明组合学的优美和简洁性. 此外，在他教得如此之好的课程中，他一直寻求组合学主题一致性的证明. 我们谨以此书献给我们的朋友 Herb Ryser，我们敬佩他并且从他那里学到许多.

1988～1989 学年，本书的两位作者一起讲授“数学 121”课程，并开始着手写这本书. 我们的目的不仅是按照 Ryser 的风格显示看似不相关的组合学领域之间的许多联系，而且也试图在一定程度上通观整个学科. 我们的意图是使经过这一课程学习的学生，在尔后参加“组合学”的学术会议时，不会由于不熟悉论题而对讨论的问题困惑不解，因为他们至少以前在课程中已听过许多术语. 我们确信学习组合学的学生应了解组合学的尽可能多的分支.

当然，书中没有一章的内容能对标题所示的主题进行完整的论述，而只是包括一些要点——在每一个论题中我们坚持处理一些本质的或非平凡的材料. 我们认为学习组合学的一个好的途径是间断性地多次重复主题. 由于这个原因，一些领域在本书的多个部分出现. 例如，偏序集和码出现过几次，而计数问题和图论遍及全书. 有些论题我们讲述得较详细(由于我们的喜爱)，有些材料(如范德瓦尔登积和式猜想的证明)在这里是第一次出现于教科书中.

学过一门近世代数的课程对学习本书就足够了，但并非绝对需要，对相当多内容的理解只需对数学有一定程度的了解. 事实上，组合学以“容易入门”而著称，但是读者会发现本书带来的挑战以及期待填补的细节(我们希望它们既有启发性又不太难). 顺便提一句，在学习一门课程时，我们相信教师是不可代替的. 对一些专题，熟悉微积分、群、有限域、初等数论，尤其是线性代数是必需的. 在加州理工学院，学习这一课程的既有本科生又有研究生. 每一章的材料都在课堂上讲授过，但我们从来没有在一学年中讲完全书.

每章后面的评注通常包含对数学家的传记性评论，在选择时我们不提及在世的数学家，除非他们已退休(P. Erdös 除外).

练习题的难度各异，对一些问题可能需要查看附录 1 中的提示. 附录 2 给出了形式幂级数的一个简要讨论.

本书的原稿由两位作者用 $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX 排版.

J. H. v. L. , R. M. W.

埃因霍温和帕萨迪纳，1992 年

# 第 2 版前言

我们的书受到了好评，许多院校把它用作组合数学的多种形式的教材，这鼓励我们出版本书的第 2 版. 在第 2 版中，增加了新的内容和参考文献，并改正了一些拼写错误和其他一些错误.

这些新的内容中，大部分插入到前一版具有相同标题的章节里. 一个例外是，把前一版后面关于图论的两章重新组织为 4 章. 增加的内容包括 Lovász 筛法的讨论、结合区组设计，以及图的目录染色(list coloring)等.

我们增加了许多新的问题，希望这一变化可增加本书作为教科书的价值. 我们的目的不是指出书中各种问题的难度，而是再次说明问题难度可能变化很大. 难度常常是与读者的经验和背景有关的，教师需要为学生选取适当的习题. 我们喜欢本书中描述问题的思想，把最相关的问题联系起来，在每一章末尾也增加了一些问题. 每一章开始时出现的问题，未必比后面的问题容易. 附录 1 中的一些提示和评论已做了改进.

第 2 版的准备工作，是由第一作者作为 Moore 特别学者在加州理工学院的六个月访问期间完成的，感谢 Moore 基金的支持.

本书介绍组合数学中的基础理论和实际应用，讲述的内容非常广泛，讨论的问题涵盖组合数学所涉及的绝大部分领域. 本书不仅包含了通常组合数学教科书中的经典内容，而且收集了若干新的内容，如 Lovász 筛法、范德瓦尔登积和式猜想、结合区组设计、码和设计等.

本书阐述深入浅出，简明易懂，适合作为高等院校高年级本科生与低年级研究生的组合数学课程教材，也适合作为数学和其他学科的研究人员的参考书.

J. H. van Lint and R. M. Wilson: A Course in Combinatorics, Second Edition(ISBN 0-521-00601-5).

Originally published by Cambridge University Press in 1992, 2001.

This Chinese edition is published with the permission of the Syndicate of the Press of the University of Cambridge, Cambridge, England.



**本书版权登记号：图字：01-2004-1208**

**图书在版编目(CIP)数据**

组合数学教程(原书第2版)/(荷)范林特(van Lint, J. H.), (美)威尔森(R. M. Wilson)著；刘振宏，赵振江译. —北京：机械工业出版社，2007.4

(华章数学译丛)

书名原文：A Course in Combinatorics, Second Edition

ISBN 978-7-111-20595-1

Ⅰ.组… Ⅱ.①范… ②威… ③刘… ④赵… Ⅲ.组合数学-教材 Ⅳ.O157

中国版本图书馆 CIP 数据核字(2006)第156040号

机械工业出版社(北京市西城区百万庄大街22号　邮政编码　100037)

责任编辑：迟振春

北京牛山世兴印刷厂印刷 · 新华书店北京发行所发行

2007年4月第1版第1次印刷

186mm×240mm · 23.75印张

定价：49.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：(010)68326294

# 目　录

# 第1章　图

一个图 $G$(graph)由顶点(vertex)集 $V$(或 $V(G)$)、边(edge)集 $E$(或 $E(G)$)，以及联系每一边 $e\in E(G)$的顶点无序对 $x$，$y$(即 $e$ 的两个端点)的映射组成. 我们称一边关联于它的端点，亦称边连结它的端点. 允许一边的两个端点 $x$ 和 $y$ 相同，即 $x=y$，称这样的边为环(loop). 当一个顶点不关联于任何边时，称它为孤立点(isolated vertex).

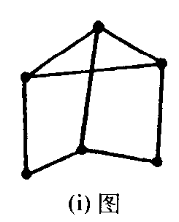
表示一个图的通常方法是把它画在平面上，用点表示顶点，用点对之间的线段或弧表示边. 例如，人们可以认为是城市之间的道路网络. 如果一个图能画在平面上，使它的任何两条边不交叉(这里是用线段或弧表示边)，则称这个图是平面的(planar). 在第 33 章里将讨论图的平面性专题，这里仅从纯组合意义上讨论图.

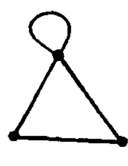
| 边 | 端点 |
|---|---|
| $a$ | $x$, $z$ |
| $b$ | $y$, $w$ |
| $c$ | $x$, $z$ |
| $d$ | $z$, $w$ |
| $e$ | $z$, $w$ |
| $f$ | $x$, $y$ |
| $g$ | $z$, $w$ |

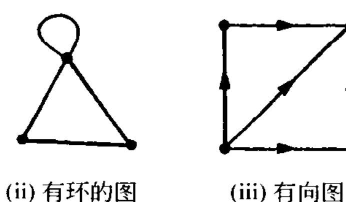
图 1.1

1

于是，可以用一个表来描述一个图，如图 1.1 中的表，列出了每一边的两个端点. 这个表所描述的图的顶点集为 $V=\{x, y, z, w\}$，边集为 $E=\{a, b, c, d, e, f, g\}$，这个图的一种画法如图 1.2(iv)所示.


(i) 图


(ii) 有环的图


(iii) 有向图

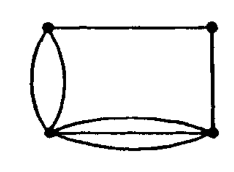

(iv) 有重边的图

图 1.2

一个图，如果它没有环并且没有相同的端点对之间有两条不同的边，则称这个图为简单的(simple). 当两个非环的边有相同的端点时，称它们是平行的. 含有平行边的图称为多重图(multigraph)或者有重边的图.

如果联系每一条边的顶点对是有序的，则称这个图为有向图(directed graph 或 digraph). 有向图的画法是，从关联边的有序对的第一个顶点(尾)向第二个顶点(头)画一个箭头. 对于简单有向图，是指它不含环且相同的顶点对间没有两条不同的边.

在讨论简单图时，通常用边连接的顶点无序对表示边，即连接 $x$ 和 $y$ 的边可以用$\{x, y\}$表示. 类似地，简单有向图的边可以用不同顶点的有序对$(x, y)$表示.

画同一个图有多种方法. 例如，图 1.3 中的两个图本质上是相同的.

下面给出更确切的描述，为避免不必要的类同的定义，我们只对无向简单图给出两个定义.

两个图称为是同构的(isomorphic)，如果它们的顶点集之间存在 1-1 对应，使得一个图中的两个顶点由一边连结，在另一个图中对应的两个顶点也由一边连结. 为了说明图 1.3 中的两个图是相同的，给这两个图的顶点适当标号(用 1，2，3，4，5，6 标号)，可以发现两个边集有相同的无序对集合.

2

图 $G$ 的顶点集上的一个置换 $\sigma$ 称为是 $G$ 的一个自同构，若 $\sigma$ 具有性质：$\{a, b\}$ 是边当且仅当 $\{\sigma(a), \sigma(b)\}$ 是边.

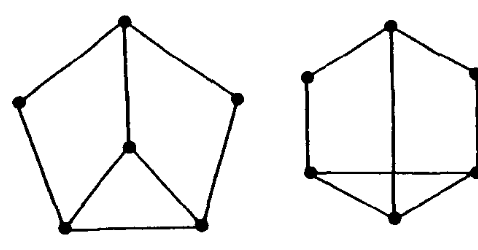


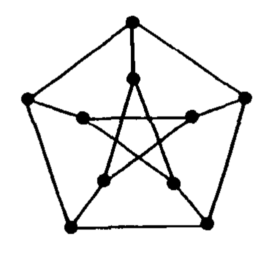
图 1.3

**问题 1A** (i)证明图 1.4 中画的两个图是相同的图(或同构图).

(ii)找出图 1.4 中图的自同构群.

**注记** 没有一种快速简易的方法去找出一个图的自同构群，除非你有好运气，因此不得不去试验各种可能性.

$n$ 个顶点的完全图(complete graph) $K_n$ 是一个有 $\binom{n}{2}$ 条可能边的简单图.



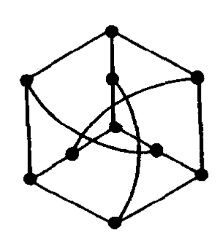


图 1.4

一个图的两个顶点 $a$ 和 $b$ 称为是相邻的(adjacent)，如果这两个顶点是不同的并且由一边连结它们. 我们用 $\Gamma(x)$ 表示与顶点 $x$ 相邻的所有顶点集合，这些顶点也称为 $x$ 的邻点.

3

关联于顶点 $x$ 的边数，称为 $x$ 的次(degree)或价(valency). 由图可见，环对价的贡献为 2. 如果一个图的所有顶点的次均相同，则称这个图为正则的(regular).

组合数学中的重要工具之一是以两种不同的方式计算某对象数量的方法. 众所周知，若人们不犯错误，那么这两种计数方法所得答案是相同的. 我们给出第一个基本例子. 一个图 $G$，若 $E(G)$ 和 $V(G)$ 都是有限集，则称 $G$ 为有限图. 我们将主要关心有限图，甚至可能偶然地出现这种情况，即在某些结论的假设中，忘记了有限图的要求.

**定理 1.1** 任一个有限图有偶数个奇价顶点.

**证明** 像图 1.1 中一样，把边的端点列成一个表，表的右列中元素的个数等于边数的两倍. 另一方面，按次的定义，顶点 $x$ 的次是 $x$ 在表中出现的次数. 因此右列中的元素个数为

$$\sum_{x \in V(G)} \deg(x) = 2 \mid E(G) \mid . \tag{1.1}$$

由此直接可得结论. ■

式(1.1)很简单，但很重要. 它可以称为图论的"第 1 定理"，我们的定理 1.1 是其第 1 推论.

一个图 $G$ 的子图(subgraph)是一个图 $H$，使得 $V(H) \subseteq V(G)$，$E(H) \subseteq E(G)$，并且边 $e \in E(H)$ 的端点与它在 $G$ 中的端点相同. 当 $V(H) = V(G)$ 时，$H$ 称为支撑子图(或生成子图). 由图 $G$ 的顶点子集 $S$ 诱导的 $G$ 的子图，是指这样一个子图，它的顶点集为 $S$，边集是 $G$ 中两个端点均在 $S$ 中的所有边之集合.

图 $G$ 的一条步路是顶点和边的交错序列

4

$$x_0, e_1, x_1, e_2, x_2, \cdots, x_{k-1}, e_k, x_k,$$

其中诸 $x_i$ 不必不同，而每一边 $e_i$ 的两个端点恰是 $x_{i-1}$ 和 $x_i$，$i=1, 2, \cdots, k$. 这样一条步路(walk)的长度为 $k$. 如果这个图是简单的，那么一条步路由它的顶点交错序列确定，这个序列里任两个相继的元素相邻.

如果这些边的项 $e_1$，$e_2$，…，$e_k$ 都是不同的，那么这条步路称为从 $x_0$ 到 $x_k$ 的**路**. 如果 $x_0=x_k$，那么这条步路(或路)称为**闭的**. 一条**简单路**就是所有顶点 $x_0$，$x_1$，$x_2$，…，$x_k$ 都不同的步路，当 $k\geqslant1$ 且除 $x_0=x_k$ 外所有顶点均不同时，称它为**简单的闭路**.

如果对于 $G$ 的每一对顶点 $x$，$y$，都存在从 $x$ 到 $y$ 的路，则称 $G$ 是**连通的**(connected). 否则 $G$ 由一些**连通分支**(极大连通子图)组成. 为了方便，约定没有顶点也没有边的空(null)图是不连通的.

**问题 1B** 假设 $G$ 是有 10 个顶点的简单图且不连通，证明 $G$ 最多有 36 条边. 能恰有 36 条边吗?

如果从 $a$ 到 $b$ 存在步路，那么从 $a$ 到 $b$ 的最短步路的长度称为这两个顶点间的**距离** $d(a,b)$. 这样的最短步路一定是简单路.

**例 1.1** 一个有名的图是把世界上的数学家作为顶点，两个顶点相邻当且仅当对应的两个数学家发表过合作的论文. 在这个图中，从一个数学家到顶点 P. Erdös 的距离称为他(她)的埃德斯(Erdös)数.

一个**多边形**就是一条简单闭路的图，更确切地说，它可以定义为次为 2 的正则连通有限图. 对每一个正整数 $n$，在同构意义上恰有一个 $n$ 个顶点的多边形 $P_n$(通常称为 $n$-边形). 图 1.5 中表示出了一系列的多边形.

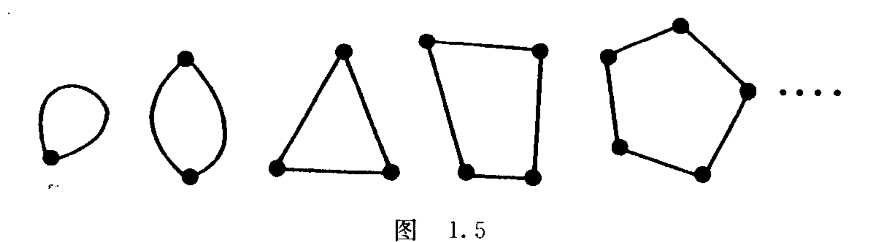


图 1.5

不含有简单闭路，即不含子图为多边形的连通图称为**树**(tree).

**问题 1C** 证明 $n$ 个顶点的连通图是树，当且仅当它有 $n-1$ 条边.

**问题 1D** 完全二部图 $K_{n,m}$ 有 $n+m$ 个顶点 $a_1$，$a_2$，…，$a_n$ 和 $b_1$，$b_2$，…，$b_m$，并且所有 $mn$ 个顶点对 $\{a_i, b_j\}$ 为其边. 证明 $K_{3,3}$ 不是平面图.

每一本图论的入门书，都不可能没有哥尼斯堡(Königsberg，从前是 Prussia 的一座城)桥问题. Pregel 河穿过这座城，并把城分为两部分. 在这条河里有一个 Kneiphof 岛. 有七座桥连接该城的两部分，如图 1.6 所示.

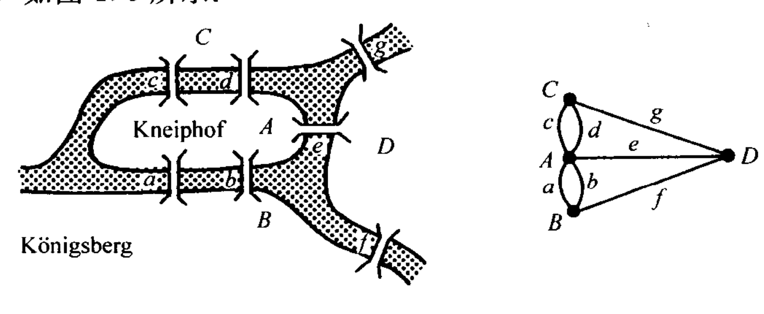



图 1.6

1736年欧拉(L. Euler)在一篇文章(被认为是图论的第一篇文章)里断言下述问题是困难的：存在一条步路经过每座桥一次且仅一次而回到出发点吗？这篇文章导出了下述定义．通过图中每一条边一次且仅一次的闭路称为欧拉回路，有这样的路的图称为欧拉图．

5～6

**定理 1.2** 没有孤立顶点(但允许有重边)的有限图 $G$ 是欧拉的，当且仅当它连通且每一顶点是偶次的．

**证明** $G$ 必须连通是显然的．因为这样的路通过某一边进入一顶点，然后通过另一边离开这个顶点．因此所有顶点的次显然必定是偶数．为了证明条件的充分性，我们从一个顶点 $x$ 出发构造一条路．在保证同一边不使用两次的情况下，继续延长这条路，直到不能再进一步延长为止．因为每一个顶点都是偶次的，所以只有回到顶点 $x$，并且关联于 $x$ 的边都已用完时才能出现这种情况．若图中还有没使用过的边，那么考虑由未使用过的边构成的子图．我们用同样的方法构造这个子图的分支的路，这样就得到第二条闭路，如果第二条闭路的一个点出现在第一条路上，那么这两条路合起来就得到从 $x$ 到 $x$ 的一条更长的路，继续这个过程．因此，这些闭路的最长者必使用了图中所有的边． ■

哥尼斯堡桥问题可以用图 1.6 中的图描述．由于没有偶次点，所以它没有欧拉回路．

对有向图可以讨论类似的问题．一个有向图有有向欧拉回路的必要和充分条件是，这个有向图连通并且每一个顶点的入次和出次相同．

**例 1.2** 一个使人为难的问题称之为"瞬时狂"(Instant Insanity)，它是将 4 个立方体的每一个面用红、蓝、绿和黄四种颜色之一染色，使得每一种颜色至少出现在每一个立方体的一个面上．问题是要把这 4 个立方体堆垒成一个 1×1×4 的长方柱，使这个长方柱 4 个侧面中每一个都恰有 4 种颜色．图 1.7 中是 4 个立方体的面染色被展平的形式．

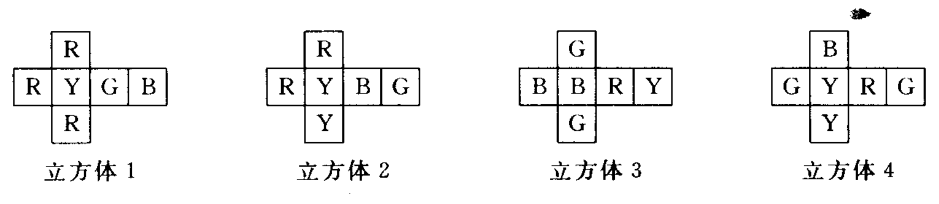



图 1.7

用试验所有可能的堆垒方式来找出答案的思想是不可取的．一个惯常的方法如下．图 1.8 中的图给出了 4 个立方体的本质信息．

7

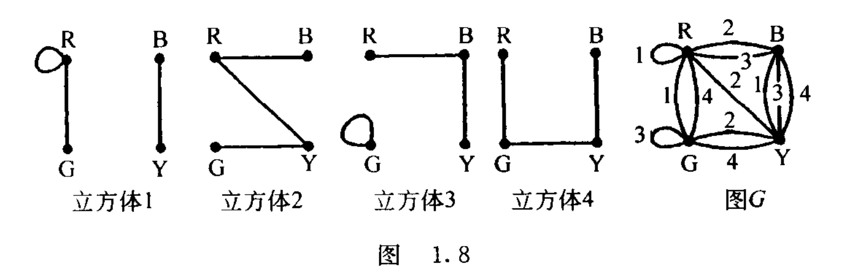



图 1.8

一条边表示立方体相对的两个面的颜色相邻．把图 1.8 中的前 4 个图叠加起来，得到图 $G$，其中 $G$ 的边上的数字，表示它是第几个立方体中的边．不难看出，我们需要找出 $G$ 的

两个没有公共边的次为 2 的正则子图，并且每一个都是由标号为 1，2，3，4 四边组成. 一个子图告诉我们堆垒的长方柱左右侧面上平行对应的颜色对，而另一个子图描述了前后侧面的颜色对. 当然很容易旋转这些立方体，使其颜色面到达所要求的位置. 这个例子的要点就是用一点时间找出上述两个子图. 这个例子的解是唯一的.

下述提到的概念似乎类似于欧拉回路，但在本质上是很不同的. 一个图 $G$ 的哈密顿回路是过 $G$ 的每一个顶点(而不是边)恰好一次的简单闭路. 因此，一个图有哈密顿回路当且仅当它有一个多边形为其支撑子图. 在 19 世纪中期，哈密顿(W. R. Hamilton)努力使得在正十二面体图上(图 1.9)寻找这样一条闭路通俗化. 8

图 1.4 中的图称为彼得森图(Petersen graph)(参见第 21 章)，这个图之所以著名，原因之一是它是非哈密顿的；对 $n=5$，6，8，9，它含有 $n$-边形，但它不含有 7-边形和 10-边形.

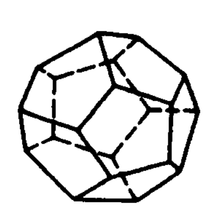
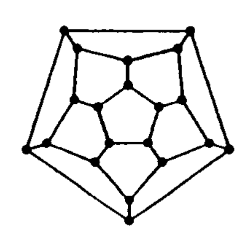



图 1.9

根据定理 1.2，很容易判断一个图是否有欧拉回路. 计算机也能容易地检查一个图的顶点次是否为偶数以及是否连通，甚至于当存在欧拉回路时，能把它找出来. 与此相反，判断一个图是否有哈密顿回路可能是“困难”的(intractable). 更确切地说，已证明这个问题是 $NP$-完全的(complete)——见 Garey and Johnson(1979).

**问题 1E** 令 $A_1$，$A_2$，…，$A_n$ 是 $n$-集 $N:=\{1, 2, \cdots, n\}$ 的不同子集. 证明存在一个元素 $x\in N$，使得集合 $A_i\setminus\{x\}(1\leqslant i\leqslant n)$ 都是不同的. 为此，在诸顶点 $A_i$ 上构造一个图 $G$，$G$ 中顶点 $A_i$ 和 $A_j$ 之间有边且染色 $x$，当且仅当 $A_i$ 和 $A_j$ 的对称差是 $\{x\}$. 现在讨论 $G$ 中一个多边形的边上的颜色. 证明能够去掉 $G$ 中的某些边，使 $G$ 中剩下的边不含多边形，并且剩下边的颜色数不变. 然后利用问题 1C 即得. (这一思想归功于 J. A. Bondy(1972).)

**问题 1F** 一个图的围长(girth)是这个图的最小多边形的边数. 设 $G$ 为围长是 5 的图，并且它的每一个顶点的次大于等于 $d$. 证明 $G$ 至少有 $d^2+1$ 个顶点. 等式能成立吗?

**问题 1G** 证明任一个有限简单图至少有两个顶点其次相同.

**问题 1H** 顶点集$\{1, 2, \cdots, n\}$上的一个图通常用一个 $n$ 阶矩阵 $A$ 来描述，其元素 $a_{ij}$ 和 $a_{ji}$ 等于两个端点分别为 $i$ 和 $j$ 的边的条数. 那么矩阵 $A^2$ 的元素的组合含义是什么?

**问题 1I** 令 $Q:=\{1, 2, \cdots, q\}$. 设 $G$ 是以 $Q^n$ 中的元素为顶点的图，并且顶点$(a_1, a_2, \cdots, a_n)$和$(b_1, b_2, \cdots, b_n)$之间有一条边当且仅当恰有一个 $i$，使得 $a_i\neq b_i$. 证明 $G$ 是哈密顿的. 9

**问题 1J** 令 $G$ 是 $n(n>3)$个顶点的简单图且没有次为 $n-1$ 的顶点. 假定 $G$ 的任两个顶点都存在唯一一个公共的邻点.

(i)证明 $G$ 的任两个不相邻的顶点 $x$ 和 $y$，都有相等的次.

(ii)证明 $G$ 是正则图.

## 评注

埃德斯(P. Erdös，1913—1996)(见例 1.1)大概是 20 世纪最多产的数学家，发表了 1400

多篇论文．他对组合学、数论、集合论等的贡献中，包含了许多重要的结论．他与世界上许多数学家合作，凡是和他合作的人都为有埃德斯数 1 而自豪，这其中也包含本书的作者；见 J. W. Grossman(1997)．

欧拉(L. Euler，1707—1783)是瑞士数学家，他一生大部分时间居住在圣彼得堡．他大概一直是多产的数学家，即使在 1766 年眼睛失明后，他仍以同样的步伐继续工作．1986 年庆祝图论诞生 250 周年，就是基于欧拉关于哥尼斯堡桥问题的论文发表时而确定的．哥尼斯堡现在是俄罗斯的加里宁格勒(Kaliningrad)的一个城市．

我们推荐 R. J. Wilson(1979)以及 J. J. Watkins and R. J. Wilson(1990)这两本书，作为图论的基础入门书．

哈密顿爵士(Sir William Rowan Hamilton，1805—1865)是爱尔兰数学家．他是一个天才，12 岁时就会 13 种语言，22 岁时(尚未完成学位)在都柏林三一学院被任命为天文学教授．他的最重要工作是在数学物理方面．

## 参考文献

M. Garey and D. S. Johnson (1979), *Computers and Intractability; A Guide to the Theory of NP-completeness*, W. H. Freeman and Co.

J. W. Grossman (1997), Paul Erdős: The Master of Collaboration, pp. 467–475 in *The Mathematics of Paul Erdős*, R. L. Graham and J. Nešetřil (eds.), Springer-Verlag.

10

J. J. Watkins and R. J. Wilson (1990), *Graphs (An Introductory Approach)*, J. Wiley & Sons.

11

R. J. Wilson (1979), *Introduction to Graph Theory*, Longman.

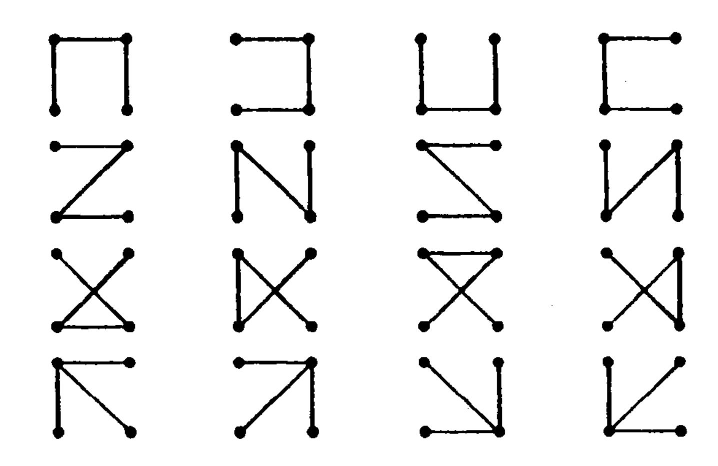
# 第2章 树

我们先来看一个不太容易的定理，它归功于 A. Cayley(1889). 本章对这个定理给出三种不同的证明. 还有两个证明放在后面的章节里，见例 14.14 和例 38.2. 前两个证明所使用的方法，是组合学中常用的. 要直接计算某些对象的数目似乎很困难，为此人们寻找一个 1-1 映射，把难计算数目的对象集映射到较容易确定其数目的对象集.

**定理 2.1** *$n$ 个顶点的不同标号树有 $n^{n-2}$ 棵.*

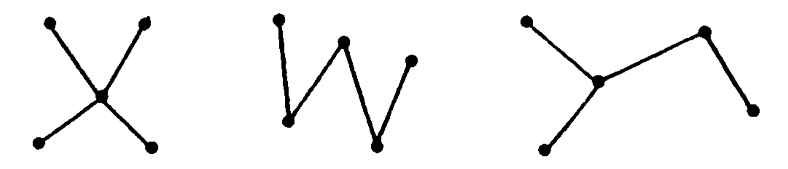
术语标号主要是强调不识别同构的图. 我们固定顶点集，两棵树是相同的，当且仅当任两个顶点在一棵树里相邻，在另一棵树里也相邻. 一个连通图 $G$ 的*支撑树*，就是 $G$ 的一个支撑子图并且它是一棵树. 这个定理可叙述为：完全图 $K_n$ 有 $n^{n-2}$ 棵支撑树.

**例 2.1** 下图是 4 个顶点上的 16 棵标号树.





**例 2.2** 下图是 5 个顶点上的 3 棵非同构的树.



$K_5$ 的支撑树中同构于一棵给定的 5 个顶点的树 $T$ 之数目，等于 5! 除以 $T$ 的自同构群的阶. (为什么?)因此，$K_5$ 有 5!/4! =5 棵树同构于上图的第 1 棵树；有 5!/2=60 棵树同构于第 2 棵树，也有同样多的树同构于第 3 棵树，$K_5$ 总共有 125 棵支撑树.

**问题 2A** 找出 6 个顶点的不同构的 6 棵树，然后对每一棵树，算出 $K_6$ 有多少支撑树同构于它.

证明之前，我们先观察下述事实. (在解问题 1C 时，读者大概已注意到了.)首先，对每一棵有 $n\geqslant 2$ 个顶点的树，至少有两个一价顶点(次为 1 的顶点). 这是显然的，如由问题 1C 和式(1.1)可见：每一个顶点的次至少为 1，这 $n$ 个顶点的次 $d_1$，$d_2$，…，$d_n$ 之和为 $2n-2$. 其次，若去掉一棵树的一个一价顶点及其关联的边，剩下的图仍是一棵树. 最后，给定一棵树

$T$，如果增加一个新顶点 $x$ 及连接 $x$ 到 $T$ 的任一顶点的一条边，那么得到的新图仍是一棵树.

**证明 1** 我们给出的第一个证明，归功于 H. Prüfer(1918)，这是一个算法，联系于任一棵
13
树 $T$，有一个刻画这棵树特征的名字 $\mathcal{P}(T)$(称为普吕弗(Prüfer)码).

对 $K_n$ 的顶点取为有序集 $V=\{1, 2, 3, \cdots, n\}$. 给定 $K_n$ 的一棵支撑树 $T$，令 $T_1=T$，并且生成树的一个序列 $T_1, T_2, \cdots, T_{n-1}$，及顶点的两个序列如下：给定 $n-i+1$ 个顶点的树 $T_i$，$i=1, 2, \cdots, n-1$，令 $x_i$ 是 $T_i$ 的最小的一价顶点，从 $T_i$ 中去掉 $x_i$ 及其关联边 $\{x_i, y_i\}$，这样就得到了 $n-i$ 个顶点的树 $T_{i+1}$. $T$ 的名字为

$$\mathcal{P}(T)=(y_1, y_2, \cdots, y_{n-2}).$$

我们断定映射 $\mathcal{P}$ 是从 $K_n$ 的所有支撑树集合到所有可能的名字的集合 $V^{n-2}$，是 1-1 的满射(双射). 这样就证明了 $K_n$ 的支撑树的数目为 $n^{n-2}$.

对于图 2.1 中的树，其中 $n=10$，有 $(x_1, y_1)=(3, 2)$，$(x_2, y_2)=(4, 2)$，$(x_3, y_3)=(2, 1)$，$\cdots$，$(x_9, y_9)=(9, 10)$；这些边就是下述矩阵的列.

$$\begin{bmatrix} 3 & 4 & 2 & 5 & 6 & 7 & 1 & 8 & 9 \\ 2 & 2 & 1 & 1 & 7 & 1 & 10 & 10 & 10 \end{bmatrix}$$

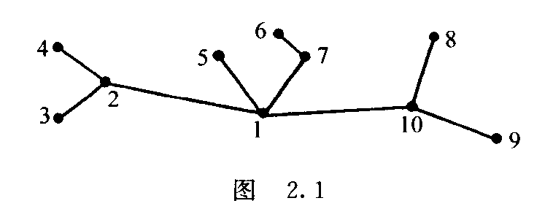


图 2.1

因此 $\mathcal{P}(T)=(2, 2, 1, 1, 7, 1, 10, 10)$，不包含 $y_9=10$.

为了理解为什么 $\mathcal{P}$ 是双射，我们首先注意关于诸 $x_i$ 和 $y_i$ 的几个简单的事实. 首先 $y_{n-1}=n$. 这是因为每一棵(至少有两个顶点的)树至少有两个一价顶点，所以顶点 $n$ 永远不会是最小的一价顶点. 其次，$x_k, x_{k+1}, \cdots, x_{n-1}$ 和 $n$ 都是树 $T_k$ 的顶点. 最后，对 $k\leqslant i\leqslant n-1$，$\{x_i, y_i\}$ 按某一顺序都是 $T_k$ 的边.

一个顶点 $v$ 在 $y_1, y_2, \cdots, y_{n-2}$ 中出现的次数等于 $\deg_T(v)-1$. 这是由于顶点 $v$ 在诸边 $\{x_i, y_i\}(1\leqslant i\leqslant n-1)$ 中出现 $\deg_T(v)$ 次，并且恰有一次出现在 $x_1, x_2, \cdots, x_{n-1}, y_{n-1}$ 里. 类似地，$T_k$ 的一个顶点 $v$ 在 $y_k, y_{k+1}, \cdots, y_{n-2}$ 中出现的次数等于 $v$ 在树 $T_k$ 中的次减 1. 特别是，$T_k$ 的一价顶点就是 $V$ 中不在集合

$$\{x_1, x_2, \cdots, x_{k-1}\} \cup \{y_k, y_{k+1}, \cdots, y_{n-1}\}$$

中的那些顶点，这就意味着 $T_k$ 的最小一价顶点 $x_k$ 是集合 $\{1, 2, \cdots, n\}$ 中不在上述集合里的
14
最小元素. 具体地说，$x_1$ 是 $V$ 中不在名字 $\mathcal{P}(T)$ 里的最小元素，并且我们能由 $\mathcal{P}(T)$ 和 $x_1, x_2, \cdots, x_{k-1}$ 唯一地确定 $x_k$. ■

**问题 2B** 顶点集为 $\{1, 2, 3, 4, 5, 6, 7\}$ 的所有树中，有多少满足下述条件的树？顶点 2 和 3 的次为 3，顶点 5 的次为 2，其余顶点的次为 1. 不要只画图，而要讨论这些树的普吕弗码.

**证明 2** 我们用一个可逆算法再给出另一个证明. 考虑从 $\{2, 3, \cdots, n-1\}$ 到 $\{1, 2, 3, \cdots, n\}$ 的一个映射 $f$，这样的映射 $f$ 有 $n^{n-2}$ 个. 由映射 $f$ 构造顶点集 $\{1, 2, \cdots, n\}$ 上的一个有向图 $D$，$D$ 的边由 $(i, f(i))$ 定义，其中 $i=2, \cdots, n-1$. 图 2.2 表示了 $n=21$ 的一个例子.

$D$ 由根为 1 和 $n$ 的两棵树及一些(如 $k$ 个)回路(有向多边形)上挂了若干树组成.（一有向树的所有边的方向都指向一个顶点，这个顶点称为根，而有向树也称为树形图.）这些回路像

图 2.2 中那样排列，其第 $i$ 个分支最右边的顶点用 $r_i$ 表示，它是回路上的最小元素（用 $l_i$ 表示最左边的顶点）. 这些回路的排放次序为 $r_1<r_2<\cdots<r_k$. 加进边 $\{1, l_1\}$, $\{r_1, l_2\}$, $\cdots$, $\{r_{k-1}, l_k\}$, $\{r_k, n\}$ 把这些分支粘连起来，再去掉边 $\{r_i, l_i\}$ 就得到一棵树. 如图 2.3 所示.

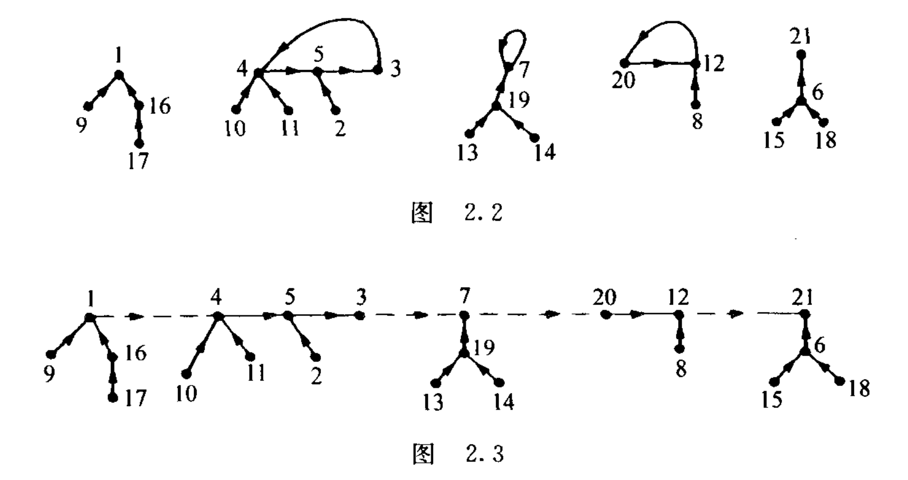


图 2.2

图 2.3

如果给定图 2.3 中的树，考察从 1 到 $n$ 的路（这里 $n=21$）. 令 $r_0:=1$. 定义 $r_1$ 是这条路上最小的数（除 $r_0=1$ 外），一般地，取 $r_i$ 为从 $r_{i-1}$ 到 $n$ 的路上最小的数. 容易看出，按照这种方法我们就把映射 $f$ 恢复出来. ■ 15

这个证明的一些推广，见 Eğecioğlu and Remmel(1986).

**问题 2C** 令 $G$ 是一个有向图且有（有向的）欧拉回路，$G$ 的顶点为 $x_1$, $x_2$, $\cdots$, $x_n$. 以 $x_i$ 为根的支撑树形图是 $G$ 的以 $x_i$ 为根的支撑树 $T$，使得对一切 $j\neq i$，在 $T$ 中自 $x_j$ 到 $x_i$ 有一条有向路. 证明 $G$ 中以 $x_i$ 为根的支撑树形图的个数不依赖于 $i$.（这是一个困难问题，参见提示.）

**证明 3** 我们现在给出用直接计算的证明，理解这种方法是很有用的. 我们提醒读者注意多项式系数的定义. 令 $r_1$, $r_2$, $\cdots$, $r_k$ 是和为 $n$ 的非负整数，那么 $\binom{n}{r_1,\ \cdots,\ r_k}$ 是由

$$(x_1+x_2+\cdots+x_k)^n=\sum\binom{n}{r_1,\ \cdots,\ r_k}x_1^{r_1}x_2^{r_2}\cdots x_k^{r_k} \tag{2.1}$$

确定的，其中是对一切和为 $n$ 的 $k$-元有序组 $(r_1, \cdots, r_k)$ 求和.

因为 $(x_1+\cdots+x_k)^n=(x_1+\cdots+x_k)^{n-1}(x_1+\cdots+x_k)$，我们有

$$\binom{n}{r_1,\cdots,r_k}=\sum_{i=1}^{k}\binom{n-1}{r_1,\cdots,r_i-1,\cdots,r_k}. \tag{2.2}$$

用 $t(n; d_1, d_2, \cdots, d_n)$ 表示 $n$ 个顶点其次为 $d_1$, $d_2$, $\cdots$, $d_n$ 的标号树的个数. 显然，如果某个 $d_i=0$，则这个数为 0. $t(n; d_1, d_2, \cdots, d_n)$ 的值只依赖于诸 $d_i$ 的多重集，而不依赖于它们之间的次序. 不失一般性，我们假定 $d_1\geqslant d_2\geqslant\cdots\geqslant d_n$，因此 $d_n=1$. 取顶点 $v_n$ 对应于 $d_n$. 把 $v_n$ 用一条边连接到某个次 $d_i\geqslant 2$ 的顶点 $v_i$，并且余下的任一个顶点都是候选的. 因此 16

$$t(n;d_1,\cdots,d_n)=\sum_{i=1}^{n-1}t(n-1;d_1,\cdots,d_i-1,\cdots,d_{n-1}). \tag{2.3}$$

对 $n=3$，很容易验算下式成立：

$$t(n;d_1,\cdots,d_n)=\binom{n-2}{d_1-1,\cdots,d_n-1}. \tag{2.4}$$

由于式(2.4)的左端和右端的数，都满足相同的递推关系(分别是式(2.3)和式(2.2))，故由归纳法就证明了对一切 $n$，式(2.4)成立. 在式(2.1)里我们用 $n-2$ 替代 $n$，用 $n$ 替代 $k$，用 $d_i-1$ 替代 $r_i$，用 1 替代 $x_i$，得到

$$n^{n-2}=\sum t(n;\ d_1,\ d_2,\ \cdots,\ d_n).$$

■

由式(2.4)能得到问题 2B 的解.

用下述方法容易构造一棵支撑树：从任一顶点开始，取到这些顶点距离为 1 的边，然后取到每一顶点距离为 2 的一条边，等等. 构造支撑树还有其他一些方法(例如，从 $G$ 开始逐一去掉 $G$ 的一些适当的边).

一个图，若不含多边形为其子图，则称它为**森林**(forest). 一个森林 $G$ 的每一个分支 $C_1$，$C_2$，…，$C_k$ 都是一棵树. 因此，如果一个森林有 $n$ 个顶点 $k$ 个分支，则它有

$$(|V(C_1)|-1)+(|V(C_2)|-1)+\cdots+(|V(C_k)|-1)=n-k$$

条边.

一个**赋权图**就是每一边 $e$ 有一个(通常非负)实数 $c(e)$的图，这些实数称为边的**长度**或**费用**等. 这里我们称它们为"费用". 设 $G$ 是一个赋权的连通图，$G$ 的一棵支撑树 $T$ 的**费用**定义为

17

$$c(T):=\sum_{e\in E(T)}c(e).$$

图可以表示城市间的网络，其中 $c(\{x,\ y\})$为城市 $x$ 和 $y$ 间架设电话线的费用. 显然，求 $G$ 的最便宜的支撑树是一个有用的重要问题.

下述方法通常称为**贪心**(greedy)**算法**. 实际上，它只是若干个贪心算法中的一个. 这个算法没有预先的计划，也不需瞻前顾后，而是在每一次都随意地选取看起来是最好的一个. 使人惊奇的是，这样一种简单的方法实际上能得到最便宜的支撑树，其证明见下述定理 2.2. 图 $G$ 的边的一个子集 $S$，若 $S$ 的支撑子图(用 $G:S$ 表示)是一个森林，那么我们称 $S$ 是**独立的**.

**贪心算法** 令 $G$ 是 $n$ 个顶点的连通图赋权图. 在每一步，我们有 $i$ 条独立边的集合$\{e_1,\ e_2,\ \cdots,\ e_i\}$(开始时 $i=0$)，使得 $G:\{e_1,\ e_2,\ \cdots,\ e_i\}$有 $n-i$ 个分支. 若$i<n-1$，令 $e_{i+1}$是这样一条边，它的两个端点在 $G:\{e_1,\ e_2,\ \cdots,\ e_i\}$的两个不同的分支里，并且在所有这样的边中，它的费用最小. 当我们已选取 $n-1$ 条边时，算法就终止.

**定理 2.2** 设上述算法选取的边集为$\{e_1,\ e_2,\ \cdots,\ e_{n-1}\}$，则支撑树 $T_0:=G:\{e_1,\ \cdots,\ e_{n-1}\}$具有下述性质：对 $G$ 的任意支撑树 $T$，有 $c(T_0)\leqslant c(T)$.

**证明** 令$\{a_1,\ a_2,\ \cdots,\ a_{n-1}\}$是树 $T$ 的边集合，并且其编号满足 $c(a_1)\leqslant c(a_2)\leqslant\cdots\leqslant c(a_{n-1})$. 我们断言有比 $c(T_0)\leqslant c(T)$更强的结论，即对一切 $i=1,\ 2,\ \cdots,\ n-1$ 有 $c(e_i)\leqslant c(a_i)$. 如若不然，那么存在某个 $k$，使

$$c(e_k)>c(a_k)\geqslant c(a_{k-1})\geqslant\cdots\geqslant c(a_1).$$

因为在选 $e_k$ 时，边 $a_1,\ a_2,\ \cdots,\ a_k$ 不予考虑，这就意味着这 $k$ 条边中每一条边的两个端点在 $G:\{e_1,\ e_2,\ \cdots,\ e_{k-1}\}$的同一个分支里. 因此，$G:\{a_1,\ a_2,\ \cdots,\ a_k\}$的分支数至少是$G:\{e_1,$

$e_2$，…，$e_{k-1}$}的分支数 $n-k+1$，这就与{$a_1$，$a_2$，…，$a_k$}是独立集矛盾. ■

**问题 2D** 上述贪心算法的一个变种如下：令 $x_1$ 是 $n$ 个顶点的赋权连通图 $G$ 的一个顶点，$T_1$ 是由 $x_1$ 且无边构成的子图. 当树(子图)$T_k(k<n)$定义后，在所有一个端点在$V(T_k)$里另一个端点不在 $V(T_k)$里的边中，选一条最便宜的边，记为 $e_k$，将 $e_k$ 及其 $e_k$ 不在 $V(T_k)$中的端点一起加到 $T_k$ 中，则得到新的树 $T_{k+1}$. 证明 $T_n$ 是 $G$ 的最便宜的支撑树. [18]

在许多情况下，需要从树的一个具体顶点出发搜索这棵树.（具有特殊顶点的树，称为有根树，这个特殊顶点称为树的根). 有两种众所周知的方法，称之为深度优先搜索法和广度优先搜索法. 我们用图 2.4 中的例子来说明这两种方法.

在自 $a$ 开始的深度优先搜索法中，实质上把这棵树视为围墙，沿着围墙走且保持围墙在你的左侧，即路线为 $abdidjdbebfk\cdots lhca$. 如果相应于这个搜索给顶点标以数字，那么标的数为$a=1$，$b=2$，$d=3$，$i=4$，…，$l=12$. 在这种描述里，我们依赖于这棵树的平面画法，见后续.

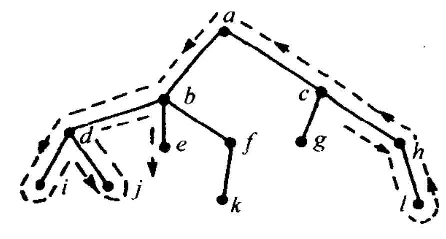


图 2.4

在广度优先搜索法中，搜索过程如同前面提到的构造支撑树的过程一样，图 2.4 中树的顶点被标数的顺序就是字母的顺序，即 $abcd\cdots jkl$.

这些思想更一般地应用于搜索一个连通图的顶点.

给定一个有限连通图$G$，按下述方法能得到$G$的顶点标号和$G$ 的一棵支撑树$T$，称之为深度优先搜索树：取一个顶点 $v_0$，并且 $T_0$ 就是由 $v_0$ 组成的树，它不含边. 归纳地，若 $T_k$ 恰是由顶点$v_0$，$v_1$，…，$v_k$ 及$G$ 的某些被选取边构成的树，在 $T_k$ 中取一顶点$v_\ell$，使$v_\ell$ 有邻点不在 $T_k$ 里并且指标 $\ell(\leqslant k)$最大. 只要 $T_k$ 不是$G$ 的支撑树，那么这样的顶点 $v_\ell$ 必存在. 当 $T_k$ 是$G$ 的支撑树时，算法终止，令 $T=T_k$. 令 $v_\ell$ 的不在 $T_k$ 中的邻点为 $v_{k+1}$，把 $v_{k+1}$和边{$v_\ell$，$v_{k+1}$}一起加到 $T_k$ 里，得到树 $T_{k+1}$. 我们把 $T$ 视为以 $v_0$ 为根的有根树. [19]

我们给出深度优先搜索树的两个性质并应用这两个性质给出关于图的定向定理的简单构造性证明.

给定以 $v_0$ 为根的有根树上的一个顶点 $x$，$x$ 的前辈(ancestor)是该树自 $x$ 到根 $v_0$ 的(唯一)路上的诸顶点. 自 $x$ 到根路上除 $x$ 外的第一个顶点，称为 $x$ 的父亲. 如果 $x$ 是 $y$ 的前辈，则称 $y$ 是 $x$ 的后代. 我们把 $x$ 也视为它自身的后代和前辈.

**命题 2.3** *如果 $x$ 和 $y$ 在 $G$ 中相邻，那么在 $G$ 的任一棵深度优先搜索树 $T$ 里，它们中的一个一定是另一个的后代.*

**证明** 在深度优先搜索中，设 $x$ 的标号比 $y$ 的标号的指标小，比如说 $x=v_k$.

当此时 $v_0$，$v_1$，$v_2$，…，$v_k$ 已被选取时，设 $v_\ell$ 相邻于一个未标号的顶点且指标 $\ell\leqslant k$ 最大，显然有 $\ell=k$. 因此在 $T$ 里 $v_{k+1}$与 $v_k$ 连结(而不是某个 $v_i$ 且 $i<k$). 如果 $v_{k+1}=y$，则结论已得证，$y$ 是 $v_k$ 的后代. 否则 $v_k$ 仍有相邻的未标号的顶点，即 $y$. 此时 $\ell$ 的选取将为 $\ell=k$ 或者 $\ell=k+1$，且 $v_{k+2}$相邻于 $T$ 中的 $v_k$ 或 $v_{k+1}$. 若 $v_{k+2}=y$，则结论已得证，$y$ 是 $v_k$ 的后代.

递归地，只要仍未标号，$v_k$，$v_{k+1}$，…，$v_{k+j}$都将是 $v_k$ 的后代，并且 $\ell$ 的下一个选取必

是 $k$，$k+1$，…，$k+j$ 中之一．然后下一个被标号的顶点 $v_{k+j+1}$ 将相邻于 $v_k$，$v_{k+1}$，…，$v_{k+j}$ 中之一，因此 $v_{k+i+1}$ 也是 $v_k$ 的后代．由于图是有限的，所以最终这个新标号的顶点必是 $y$． ■

一个连通图 $G$ 的割边(也称为桥)是 $G$ 的这样一条边，从 $G$ 中去掉这条边后就不连通了．

[20]

**命题 2.4** 令 $\{x, y\}$ 是 $T$ 的一条边，但不是 $G$ 的割边，并且 $x$ 是 $y$ 的父亲，那么 $G$ 中就存在一条边，它不在 $T$ 里并且它连结 $y$ 的某个后代 $a$ 和 $x$ 的某个前辈 $b$.

**证明** 令 $D$ 是 $y$ 的后代之集合，因此 $y\in D$ 但 $x\notin D$. 因为从 $G$ 中去掉 $\{x, y\}$ 后仍连通，所以存在某一边 $\{a, b\}\neq\{x, y\}$，使端点 $a\in D$ 而端点 $b\notin D$. 这条边 $\{a, b\}$ 肯定不在 $T$ 里，根据命题 2.3，$b$ 是 $a$ 的前辈(因为 $b$ 不可能是 $a$ 的后代，否则 $b$ 也是 $y$ 的后代，这样 $b\in D$，这与 $b\notin D$ 矛盾)．在 $T$ 中，从 $a$ 到 $v_0$ 的(唯一)路上通过 $y$($a$ 的前辈)，再过 $x$($y$ 的父亲)，而 $b$ 必须在这条路上(因为 $b$ 是 $a$ 的前辈)，因此 $b$ 也必是 $x$ 的一个前辈． ■

给一个无向图 $G$ 的每一边指定一个方向，这样就得到一个有向图，这个有向图称为 $G$ 的一个定向(orientation)．有向图 $D$ 中的一条步路称为是强的(strong)，如果步路上每一条边的方向与通过它的方向一致，即由尾到头．一个有向图 $D$ 是强连通的，如果对图中的每一对顶点 $x$，$y$，都存在自 $x$ 到 $y$ 的强步路．

**定理 2.5** 令 $G$ 是一个有限连通图且不含割边，那么 $G$ 有一个强定向．即 $G$ 的定向是一个强连通的有向图．

**证明** 利用对 $G$ 的每一边选择一个方向来构造有向图 $D$．首先找出一棵深度优先搜索树 $T$ 并对 $G$ 的顶点编号 $v_0$，$v_1$，…．令 $\{v_i, v_j\}$ 是 $G$ 的一条边且 $i<j$．如果 $\{v_i, v_j\}$ 在 $T$ 里，那给此边定向为 $v_i$ 到 $v_j$，即 $(v_i, v_j)$ 是 $D$ 的一条边．如果 $\{v_i, v_j\}$ 不在 $T$ 里，给该边定向为 $v_j$ 到 $v_i$，即 $(v_j, v_i)$ 是 $D$ 的一条边．

剩下来要证明 $D$ 是强连通的．显然从 $v_0$ 到 $G$ 的任一顶点 $x$ 存在强步路(该路由 $T$ 的边组成)，因此只要从任一顶点 $x$ 到 $v_0$ 有强步路就足够了．

给定一个顶点 $x_k$，$k>0$，命题 2.4 告诉我们 $G$ 中有某一条不在 $T$ 里的边 $\{a, b\}$，它连结 $v_k$ 的某个后代 $a$ 到 $v_k$ 的某个前辈 $b=v_i$．这样就得到 $D$ 中自 $v_k$ 到 $v_i$ 的强步路：它是 $T$ 中从 $v_k$ 到它的后代 $a$ 的强步路加上有向边 $(a, v_i)$．由于 $v_i$ 是 $v_k$ 的前辈，当然有 $i<k$．若 $i=0$，则已

[21]

证得结论．否则，重复上述的论证，找出从 $v_i$ 到某个 $v_j(j<i)$ 的强步路，再接上从 $v_k$ 到 $v_i$ 的强步路，就得到从 $v_k$ 到 $v_j$ 的强步路．按这种方法继续下去，直到到达 $v_0$ 为止．[⊖] ■

**问题 2E** $n$ 个顶点树 $T$ 的优美标号(graceful labeling)就是一个映射 $f: V(T)\to\{1, 2, \cdots, n\}$，使得对应于每一条边 $\{x, y\}$ 的数 $|f(x)-f(y)|$ 都不同．证明路图(恰有两个一价顶点的树)有优美标号．(人们猜想所有的树都有优美标号．)

**问题 2F** 假定一棵树 $G$，对 $2\leqslant i\leqslant m$ 恰有一个顶点的次为 $i$，并且所有其他顶点的次均为 1．那么 $G$ 有多少个顶点？

**问题 2G** 令 $G$ 是一个图，对 $2\leqslant i\leqslant m$，$G$ 恰有一个顶点的次为 $i$，而其余的 $k$ 个顶点的次均为 1．证明 $k\geqslant\left\lfloor\frac{m+3}{2}\right\rfloor$．给出这种图的构造．

---

⊖ 这段证明原文使用符号混乱，使读者不易看明白，译者对证明做了一些改动．——译者注

**问题 2H** 讨论具有 $2n$ 个顶点的标号三价有根树 $T$，其根标号为 $2n$，见图 14.3. 按下述方法选取标号，使得$\mathcal{P}(T)$第一行为 1，2，3，…，$2n-1$. 这种码$\mathcal{P}(T)$有多少？

## 评注

凯莱(A. Cayley，1821—1895)自 1863 年起一直到逝世都是剑桥大学教授，他是 19 世纪的伟大数学家之一. 他对椭圆形函数理论、解析几何和代数做出了重要贡献，例如不变理论. 他在 1889 年发表的关于树的文章，没有包含在我们要讨论的证明中. 在许多证明中(本书讨论了其中五个)，普吕弗的证明是最有名的.

普吕弗(H. Prüfer，1896—1934)是舒尔(I. Schur)的许多学生之一，他是芒斯特大学教授.

## 参考文献


A. Cayley (1889), A theorem on trees, *Quart. J. Pure and App. Math.* **23**, 376–378. [22]

Ö. Eğecioğlu and J. B. Remmel (1986), Bijections for Cayley trees, spanning trees, and their $q$-analogues, *J. Combinatorial Theory* (A) **42**, 15–30.

H. Prüfer (1918), Neuer Beweis eines Satzes über Permutationen, *Archiv der Math. und Phys.* (3) **27**, 142–144. [23]

# 第3章　图的染色和拉姆齐定理

我们首先看一下几个所谓的图的染色问题.

一个图 $G$ 的正常染色，是由 $G$ 的顶点集到颜色集 $C$ 的一个函数(如 $C=\{1, 2, 3, 4\}$)，使得 $G$ 的每一边的两个端点有不同的颜色(因此具有环的图没有正常染色). 如果 $|C|=k$，我们称 $G$ 是 $k$-染色的.

一个图 $G$ 的色数 $\chi(G)$ 就是使 $G$ 有正常染色的最小颜色数.

如果 $\chi(G)=2$(或者 $\chi(G)=1$，$\chi(G)=1$ 当且仅当 $G$ 没有边)，那么称 $G$ 为二部图. 读者容易验证，没有奇边形的图(等价地，不含奇长闭路的图)是二部图.

著名的"四色定理"(K. Appel and W. Haken，1977)是说，若 $G$ 是平面图，那么 $\chi(G)\leqslant 4$.

显然，$\chi(K_n)=n$. 若 $k$ 是奇数，则 $\chi(P_k)=3$. 在下述定理中，除上述这些例子外，我们证明图的色数最多等于它的最大次(R. L. Brooks，1941).

**定理 3.1**　令 $d\geqslant 3$，$G$ 是每一个顶点的次都小于等于 $d$ 的图，并且 $G$ 不含 $K_{d+1}$ 为其子图. 则 $\chi(G)\leqslant d$.

**证明 1**　如同组合分析中的许多定理的证明一样，假定定理的结论不正确，然后讨论一个极小的反例(在这个定理里就是顶点个数最小的图)，由这个反例得到矛盾，从而就证明了定理. 我们将采用重新染色的方法：能够改变某些顶点颜色，使由一种正常染色变为另外一种正常染色. 例如，令 $S$ 是颜色集 $C$ 的一个子集. 对染有 $S$ 中颜色的顶点诱导子图的任一个连通分支，我们可以对其顶点的颜色进行交换(不改变染 $C\setminus S$ 中颜色的顶点之颜色). 显然，这样可得到 $G$ 的另一种正常染色.



因此，设 $G$ 是顶点个数最小的反例. 令 $x\in G$，$\Gamma(x)=\{x_1, \cdots, x_l\}$，$l\leqslant d$. 由于 $G$ 是最小反例，那么从 $G$ 中去掉顶点 $x$ 及其关联边得到的图 $H$，必是 $d$-染色的，比如用的颜色为 1，2，…，$d$. 如果这些颜色没有在 $\Gamma(x)$ 中全部出现，那么就可以用未出现的颜色染 $x$，这样就得到 $G$ 是 $d$-染色的. 因此，必有 $l=d$，并且对 $H$ 的每一种 $d$-染色，$\Gamma(x)$ 中的顶点必占用了所有这 $d$ 种颜色. 不妨设 $x_i$ 的颜色为 $i$，$i=1, 2, \cdots, d$.

现在讨论在 $H$ 的 $d$-染色中，由颜色 $i$ 和 $j$ 染的顶点的诱导子图 $H_{ij}$. 若 $x_i$ 和 $x_j$ 分别在 $H_{ij}$ 的两个不同的连通分支中，那么我们可以在这其中的一个分支里，交换颜色 $i$ 和 $j$，这样 $x_i$ 和 $x_j$ 有相同的颜色，这是不可能的. 因此，$x_i$ 和 $x_j$ 必定在 $H_{ij}$ 的同一个连通分支里(比如 $C_{ij}$ 分支里). 我们将证明这个分支是一条从 $x_i$ 到 $x_j$ 的简单路(的图)，这条路上顶点的颜色交错为色 $i$ 和 $j$. 如果在 $H$ 中，$x_i$ 的两个邻点有颜色 $j$，那么在 $H$ 中 $x_i$ 的邻点最多占用了 $d-2$ 种颜色. 因此可以重染 $x_i$ 的颜色，这是不可能的. 假设 $y$ 是分图 $C_{ij}$ 中从 $x_i$ 到 $x_j$ 路上的第一个次大于等于 3 的顶点. 在 $H$ 中 $y$ 的邻点最多有 $d-2$ 种颜色，因此 $y$ 可以用不在 $\{i, j\}$ 中的某一颜色重新染色，这样 $x_i$ 和 $x_j$ 在 $H_{ij}$ 中不再连通了. 我们知道这是不可能的. 因此这样的 $y$ 不存在，从而证明了 $C_{ij}$ 是一条路.

假设 $z\neq x_i$ 是在两条路 $C_{ij}$ 和 $C_{ik}$ 上，那么 $z$ 有两个邻点有颜色 $j$ 且也有两个邻点有颜色 $k$.

因此在 $H$ 中 $z$ 的邻点最多有 $d-2$ 种颜色，故 $z$ 可以用不在 $\{i, j, k\}$ 中的某一颜色重染，这样得到矛盾. 因此，$C_{ij}\cap C_{ik}=\{x_i\}$.

由 $K_{d+1}\not\subseteq G$ 的假设，说明 $\Gamma(x)$ 中存在两个顶点，如 $x_1$ 和 $x_2$，使 $x_1$ 和 $x_2$ 之间没有边. 见图 3.1，顶点 $a$ 染色为 2，它是分支 $C_{12}$ 上 $x_1$ 的邻点. 25

在子图 $C_{13}$ 上交换颜色 1 和 3，这样得到 $H$ 的重新染色. 对新的染色，我们有新的路，记为 $C'_{ij}$. 显然 $a\in C'_{23}$(因为 $x_1$ 染颜色 3). 但是在 $C_{12}$ 上，除 $x_1$ 外，其他顶点颜色不变，所以 $a\in C'_{12}$. 因此，$C'_{12}\cap C'_{23}\neq\{x_2\}$，这与上述证明矛盾. 这个矛盾说明极小反例是不存在的. ■

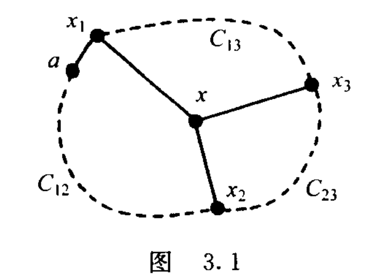


图 3.1

为布鲁克斯(Brooks)定理的第二部分证明做准备，读者在不应用这个定理的情况下，证明下述问题.

**问题 3A** 固定整数 $d\geqslant 3$. 令 $H$ 是每一个顶点的次 $\leqslant d$ 的简单图，并且 $H$ 不是 $d$-染色的顶点数最小的图(我们断定 $H$ 是 $d+1$ 个顶点的完全图，但现在还不知道这个结论).

(i)证明 $H$ 是不可分离的(即从 $H$ 中去掉任一顶点，其剩余的图仍连通).

(ii)如果将 $H$ 的顶点集 $V(H)$ 分为两部分 $X$ 和 $Y$，使 $|Y|\geqslant 3$，证明 $Y$ 中至少有三个顶点 $a$，$b$，$c$，其中每一个至少有一个邻点在 $X$ 里.

**证明 2** 令 $d$ 和 $H$ 满足问题 3A 中的假设. 若 $H$ 不是完全图，则存在顶点 $x_1$，$x_{n-1}$ 和 $x_n$，使得 $x_1$ 相邻于 $x_{n-1}$ 和 $x_n$，但这些顶点中至少有两个不相邻. 我们给剩余的 $n-3$ 个顶点编号，使得它们的顺序

$$x_1, x_2, \cdots, x_{n-1}, x_n$$

具有下述性质：对 $k\geqslant 2$，每一个 $x_k$ 至少有一个先于它的顶点 $x_i$ 与其相邻，即 $i<k$. 显然，当 $x_1$，$x_2$，…，$x_k(k<n-2)$ 已选取时，除 $x_{n-1}$ 和 $x_n$ 外，选取任一个顶点 $x_{k+1}$，使其相邻于 $x_1$，$x_2$，…，$x_k$ 中某一顶点. 由问题 3A 中的结论(ii)，至少有三个这样的顶点，所以这总是可能的. 26

当顺序排好后，我们从序列的末端开始进行 $d$-染色. 给 $x_{n-1}$ 和 $x_n$ 染相同的颜色，当最后的 $n-k$[⊖] $(k\geqslant 2)$个顶点 $x_{k+1}$，…，$x_{n-1}$，$x_n$ 已染色时，因为 $x_k$ 最多与 $x_{k+1}$，…，$x_n$ 中的 $d-1$ 个顶点相邻，所以至少还有一种颜色可染顶点 $x_k$. 最后，因为相邻于 $x_1$ 的两个顶点 $x_{n-1}$ 和 $x_n$ 有相同的颜色，所以必有一种颜色可用于染顶点 $x_1$. ■

现在我们讨论一类完全不同性质的染色问题，以此引进组合学中一个很重要的定理，称之为拉姆齐(Ramsey)定理. 在此之前，请读者尝试解决下述问题.

**问题 3B** 用红蓝两种颜色染 $K_7$ 的边，每一条边染一种颜色，证明至少有 4 个子图 $K_3$，其中每一个的边颜色相同(单色三角形). 并证明等式可以成立.

介绍这个主题，总是以红和蓝两种颜色染 $K_6$ 的边作为例子，并将证明至少有一个单色三角形. 证明如下：令 $a$ 是 $K_6$ 的任一个顶点，因为 $a$ 的次为 5，所以关联它的边中至少有三条边染相同的颜色，比如染红色，这三条边的另一端点分别为 $b$，$c$ 和 $d$. 如果这三个顶点之间的

⊖ 原文为 $k$ 个顶点，显然是不对的. ——译者注

边有一条染红色，那么我们已得到一个红色的三角形，否则，这三个顶点就构成了一个蓝色的三角形.

对于拉姆齐定理的更困难的情形，其证明思想也是相同的. 但是，它没有像下述论证表明的那么多.

**定理 3.2** 如果将 $K_n$ 的每一边染成红色或蓝色，用 $r_i$ 表示关联于顶点 $i$ 的红边的个数，$i=1, 2, \cdots, n$，用 $\Delta$ 表示单色三角形的个数，则有

$$\Delta = \binom{n}{3} - \frac{1}{2}\sum_{i=1}^{n} r_i(n-1-r_i). \tag{3.1}$$

**证明** $K_n$ 的每一个非单色三角形恰有两个顶点，它们是该三角形上红边和蓝边的交汇点. [27] 在第 $i$ 个顶点上，选取这样的两条边有 $r_i(n-1-r_i)$ 种方式. 因此，式(3.1)中的和项表示双色三角形个数的两倍. ■

**推论**

$$\Delta \geqslant \binom{n}{3} - \left\lfloor \frac{n}{2}\left\lfloor \left(\frac{n-1}{2}\right)^2 \right\rfloor \right\rfloor. \tag{3.2}$$

**证明** 由(3.1)可见，当 $n$ 是奇数且对一切 $i$ 有 $r_i=(n-1-r_i)$，或者当 $n$ 为偶数且对一切 $i$ 有 $r_i=\frac{1}{2}n$ 或 $r_i=\frac{n}{2}-1$，那么 $\Delta$ 达到最小值. 因为 $\Delta$ 是一个整数，第一种情形不可能永远出现. 因此，容易证明式(3.2)是不可能改进的. ■

注意，上述结论说明，用红蓝颜色染 $K_6$ 的边，至少有两个单色三角形.

现在讨论拉姆齐定理(Ramsey，1930).

**定理 3.3** 给定整数 $r\geqslant 1$ 和 $q_i\geqslant r$，$i=1, 2, \cdots, s$. 那么存在一个最小的正整数 $N(q_1, q_2, \cdots, q_s; r)$，它有下述性质：令 $S$ 是 $n$ 个元素的集合，将 $S$ 的所有 $\binom{n}{r}$ 个 $r$-子集划分为 $s$ 个彼此不交的子集族 $T_1, T_2, \cdots, T_s$(可视为 $s$ 种颜色)，则当 $n\geqslant N(q_1, q_2, \cdots, q_s; r)$ 时，必存在某个 $i(1\leqslant i\leqslant s)$，及 $S$ 的某个 $q_i$-子集，使得 $q_i$-子集的每一个 $r$-子集都在 $T_i$ 里.

(请读者将这个定理与前述的例子进行比较，并证明 $N(3, 3; 2)=6$.)

**证明** 我们只对 $s=2$ 给予证明. 对一般情况，只涉及一些分门别类的处理.

(a)对 $r=1$，定理显然是正确的，并且 $N(p, q; 1)=p+q-1$.

(b)对任意 $r$ 及 $p\geqslant r$，显然也有 $N(p, r; r)=p$，并且类似地，对 $q\geqslant r$ 有 $N(r, q; r)=q$.

(c)对 $r$ 进行归纳证明. 假设对 $r-1$ 定理为真. 我们现在应用结果(b)并对 $p+q$ 使用归纳法. 我们定义 $p_1=N(p-1, q; r)$，$q_1=N(p, q-1; r)$. 令 $S$ 是具有 $n$ 个元素的集合，其中 $n\geqslant 1+N(p_1, q_1; r-1)$. 用两种颜色，如红和蓝染 $S$ 的所有 $r$-子集. 如同对 $K_6$ 的证明一样，[28] 选取 $S$ 中任一个元素 $a$. 我们现在按 $X\subseteq S'$ 和 $X\cup\{a\}$ 有相同的颜色，定义 $S':=S\setminus\{a\}$ 的所有 $(r-1)$-子集的染色。根据归纳假设，$S'$ 或者包含一个 $p_1$-子集 $A$，使 $A$ 的所有 $(r-1)$-子集都是红色的，或者 $S'$ 包含一个 $q_1$-子集 $B$，使 $B$ 的所有 $(r-1)$-子集都是蓝色的. 不失一般性，设前一种情况出现. 因为 $A$ 有 $N(p-1, q; r)$ 个元素，存在两种可能性：第一种可能性是 $A$ 有一个 $q$-子集，它的所有 $r$-子集是蓝色的，此时结论已得证；另一种可能性是 $A$ 有一个 $(p-1)$-

子集 $A'$，它的所有 $r$-子集是红色的．由于 $A'\subseteq A$，所以集合 $A'\cup\{a\}$ 也有这个性质．这就证明了定理，并且我们还证明了

$$N(p,q;r)\leqslant N(N(p-1,q;r),N(p,q-1;r);r-1)+1. \tag{3.3}$$

■

当返回到用两种颜色染一个图的边($r=2$)时，就出现了式(3.3)的特殊情况：由定理证明中的(a)，我们发现

$$N(p,q;2)\leqslant N(p-1,q;2)+N(p,q-1;2). \tag{3.4}$$

**问题 3C** 在式(3.4)中，如果右端的两项都是偶数，证明其等式不可能成立．

**定理 3.4**

$$N(p,q;2)\leqslant\binom{p+q-2}{p-1}.$$

**证明** 因为 $N(p,2;2)=p$，而二项式系数满足与式(3.4)相同的关系，但它取等式，所以由式(3.4)可得出定理 3.4 的结论． ■

现在我们看一下关于 $N(p,q;2)$ 的某些已知的结果．由问题 3C，我们有 $N(3,4;2)\leqslant 9$．为了证明等式成立，我们对 $K_8$ 进行染色，使其不含红色三角形，也不含蓝色的 $K_4$．我们的做法如下：将 $K_8$ 中的顶点用 $\mathbb{Z}_8$ 中的元素编号．边 $\{i,j\}$ 染红色，当且仅当 $i-j\equiv\pm 3$ 或 $i-j\equiv 4\pmod 8$．容易验证这种染色方式满足上述要求．

**问题 3D** 应用相同的方法证明 $N(4,4;2)=18$ 和 $N(3,5;2)=14$．

借助于更多的工作，证明了下述结果：

$N(3,6;2)=18$，$N(3,7;2)=23$，$N(3,8;2)=28$，$N(3,9;2)=36$，$N(4,5;2)=25$，而 $N(p,q;2)$ 的其他情形的值尚不知道． 29

在这个 30 年来没有实质性进展的领域里，一个有意义的问题是 $N(p,p;2)$ 的渐进性质．由定理 3.4，我们知道

$$N(p,p;2)\leqslant\binom{2p-2}{p-1}\leqslant 2^{2p-2}. \tag{3.5}$$

现在我们应用组合学中经常使用的一个方法，证明 $N(p,p;2)$ 呈指数增长．因为这种方法是估计随机染色下单色 $K_p$ 出现的概率，所以通常称之为概率方法．对 $K_n$ 的每一条边染红色或蓝色，那么 $K_n$ 的边有 $2^{\binom{n}{2}}$ 种不同的染色方案．现在固定其一个子图 $K_p$，那么在 $2^{\binom{n}{2}}$ 种染色方案中，使 $K_p$ 为单色的方案有 $2^{\binom{n}{2}-\binom{p}{2}+1}$ 种．使某个 $K_p$ 是单色的，其染色方案数最多是 $\binom{n}{p}$ 倍的 $2^{\binom{n}{2}-\binom{p}{2}+1}$（因为某些染色方案可能重复计算）．因此，如果这个数$\left(\text{即}\binom{n}{p}2^{\binom{n}{2}-\binom{p}{2}+1}\right)$小于总的染色方案数$\left(\text{即 }2^{\binom{n}{2}}\right)$，则存在染色方案使没有单色 $K_p$ 出现．

应用$\binom{n}{p}\leqslant n^p/p!$ 的结论，当 $n<2^{p/2}$时，我们能找出这样的染色方案(除非是 $p=2$)，这样就证明了下述定理.

**定理 3.5** $N(p, p; 2)\geqslant 2^{p/2}$.

由式(3.5)和定理 3.5，我们有

$$\sqrt{2}\leqslant\sqrt[p]{N(p,p;2)}\leqslant 4\quad(p\geqslant 2).$$

如果人们能够证明当 $p\to\infty$时，上式的 $p$-次根有极限，那将是一件很有意义的事情.

为了给定理 3.5 相当大的改进，我们讨论对组合学的许多部分有用的概率方法. 设 $A_1$，$A_2$，…，$A_n$ 为概率空间的事件，用 $Pr[A_i]$表示事件 $A_i$ 出现的概率，与通常一样，用 $\overline{A}_i$ 表示 $A_i$ 的补，即 $A_i$ 不出现. 我们感兴趣的是 $A_i$ 表示我们不希望出现的情形，并且希望能断定所有事件 $A_i$ 不出现的概率为正的. 在某些容易计算的情形，人们可应用

[30]

$$\sum_{i=1}^{n}Pr[A_i]<1\Rightarrow\bigcap\overline{A}_i\neq\varnothing.$$

参考问题 5E. 但是，一般情况下，相当多的事件之间的相关性产生重复计算，这样就导致和项的值远大于 1. 当然，如果这些事件是独立的，那么每一事件概率小于 1 就能保证所有事件不出现的概率为正的. Lovász 筛法处理的情形中的确有某些相关性，但同时也有许多显然独立的事件组合.

对于事件 $A_1$，$A_2$，…，$A_n$，我们定义一个所谓的*相关性图*. 它是指标集$\{1, 2, \cdots, n\}$上的一个图 $G$，具有这样的性质：对每一个 $i$，事件 $A_i$ 独立于$\{A_j:\{i, j\}\notin E(G)\}$的每一个子集. 注意，它比 $A_i$ 独立于这个子集中的每一个 $A_j$ 要求的更多.

**定理 3.6** *令 $G$ 是关于事件 $A_1$，…，$A_n$ 的某个相关性图. 假设 $Pr[A_i]\leqslant p$，$i=1, 2, \cdots, n$，并且 $G$ 的每一个顶点的次$\leqslant d$. 如果 $4dp<1$，则$\bigcap\overline{A}_i\neq\varnothing$.*

**证明** 我们首先证明，对指标集的每一个子集$\{i_1, i_2, \cdots, i_m\}$有

$$Pr[A_{i_1}\mid\overline{A_{i_2}}\cdots\overline{A_{i_m}}]\leqslant\frac{1}{2d}.\tag{3.6}$$

当 $m=1$ 时，是显然的. 对 $m=2$，我们有

$$Pr[A_1\mid\overline{A_2}]\leqslant\frac{p_1}{1-p_2}\leqslant\frac{1}{4d-1}<\frac{1}{2d},$$

其中为了符号上的方便，我们取 $i_j=j$ 及 $p_i:=Pr[A_i]$. 我们进行归纳证明.

假定在 $G$ 中，1 相邻于 2，3，…，$q$ 且不相邻于 $q+1$，…，$m$. 我们有

[31]

$$Pr[A_1\mid\overline{A_2}\cdots\overline{A_m}]=\frac{Pr[A_1\overline{A_2}\cdots\overline{A_q}\mid\overline{A_{q+1}}\cdots\overline{A_m}]}{Pr[\overline{A_2}\cdots\overline{A_q}\mid\overline{A_{q+1}}\cdots\overline{A_m}]}.$$

公式中的分子(按 $G$ 的定义)最多为

$$Pr[A_1\mid\overline{A_{q+1}}\cdots\overline{A_m}]=Pr[A_1]\leqslant\frac{1}{4d}.$$

应用归纳假设，我们发现分母至少为

$$1-\sum_{i=2}^{q}Pr[A_1 \mid \overline{A_{q+1}}\cdots\overline{A_m}]\geqslant 1-\frac{q-1}{2d}\geqslant\frac{1}{2}.$$

这样就证明了式(3.6). 现在我们有

$$Pr[\overline{A_1}\cdots\overline{A_n}]=\prod_{i=1}^{n}Pr[\overline{A_i}\mid\overline{A_1}\cdots\overline{A_{i-1}}]\geqslant\left(1-\frac{1}{2d}\right)^n>0,$$

其中，对乘积中的每一项，我们用了式(3.6). ■

我们用这个方法得到了 $N(p,\ p;\ 2)$的下界.

**定理 3.7** *$N(p,\ p;\ 2)\geqslant c\cdot p\cdot 2^{p/2}$，其中 $c$ 为一个常数.*

**证明** 讨论 $K_n$ 及用两种颜色随机地染它的边，对每一个 $k$ 个顶点的集合 $S$，令 $A_S$ 表示 $S$ 上子图染成单色的事件. 我们希望证明，在所有随机染色中，至少有一种染色，它不含有 $k$ 个顶点的单色子图. 我们定义一个相关性图：使 $S$ 和 $T$ 相邻，当且仅当 $|S\cap T|\geqslant 2$，即 $S$ 和 $T$ 上的子图有一条公共边. $G$ 的次 $d$ 显然最多为 $\binom{k}{2}\binom{n}{k-2}$. 因此事件 $A_S$ 的出现概率均为 $2^{1-\binom{k}{2}}$. 由定理 3.6、斯特林公式和某些微小巧妙的处理就得到定理的结果(如果希望对 $c$ 做出估计，也可以做到). ■

我们已给出了组合学里有名的拉姆齐理论中的一些例子. 下面再提一下另一个例子，即 B. L. van der Waerden (1927)的一个定理. 这个定理说，存在一个正整数 $N(r)$，使得当 $N\geqslant N(r)$时，用红、蓝两种颜色染自 1 到 $N$ 的整数，那么这些数的集合中，存在一个长度为 $r$ 的单色的算术级数. 这个定理的一个短的(但不容易的)证明，见 Graham and Rothschild(1974). 这一领域的一般参考文献请见 R. L. Graham，B. L. Rothschild and J. L. Spencer(1980)合著的书《Ramsey Theory》. [32]

拉姆齐定理的一个有趣应用是下述引自 Erdös and Szekeres(1935)的定理.

**定理 3.8** *给定正整数 $n$，存在正整数 $N(n)$，使得当 $N\geqslant N(n)$时，平面上任意 $N$ 个点，若其中任意 3 个点不共线，就有 $n$ 个点的子集构成一个凸 $n$-边形.*

**证明** (i)首先观察，若有 $n$ 个点且其中任意 3 个不共线，那么它们构成一个凸 $n$-边形，当且仅当其中每 4 个点形成的 4-边形是凸 4-边形.

(ii)我们断言 $N(n)=N(n,\ n;\ 3)$满足要求. 令 $S$ 是平面上 $N(n)$个点的集合，给点编号，然后按下述方式给每一个三角形染红色或蓝色：如果从三角形编号小的顶点经过编号次小点再到编号大的点之路是顺时针的，则给此三角形染红色，若是逆时针则染蓝色. 于是存在 $n$-子集，使它的所有三角形是单色的，比如红色. 我们要证明，这个集合不含图 3.2 中图的构形.

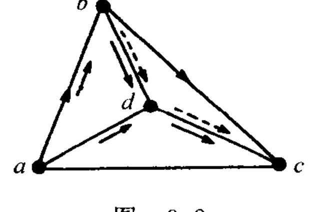



图 3.2

不失一般性，设 $a<b<c$. 由三角形 $adc$ 可得 $a<d<c$；而由三角形 $abd$ 可得 $a<b<d$. 但是三角形 $bcd$ 是蓝的，故得矛盾. 因此，由 $n$-子集中的点构成的所有 4-边形都是凸的，且根据(i)结论得证. ■

**问题 3E** $n$ 个顶点的竞赛图是 $K_n$ 的一个定向. 可迁竞赛图是这样的一个竞赛图，它的顶点能进行编号，使得$(i, j)$是边，当且仅当 $i<j$.

(a)证明，若 $k\leqslant\log_2 n$，那么每一个 $n$ 个点的竞赛图有一个 $k$ 个顶点的可迁子竞赛图.

(b)证明，若 $k>1+2\log_2 n$，则存在一个 $n$ 个顶点的竞赛图，它不含有 $k$ 个顶点的可迁子竞赛图.

33

**问题 3F** 证明对所有 $r\in\mathbb{N}$，存在一个最小的 $N(r)$，使当 $n\geqslant N(r)$时，用 $r$ 种颜色染集合$\{1, 2, \cdots, n\}$中的元素，必存在三个数 $x$，$y$，$z$(这三个数不必不同)，它们有相同的颜色，并且 $x+y=z$. (I. Schur 的结果.)求 $N(2)$. 给出 $N(3)>13$ 的初等证明.

**问题 3G** 给定正整数 $m$，证明当 $n$ 足够大时，每一个 $n\times n$ 的$(0, 1)$-矩阵有一个 $m$ 阶的主子矩阵，使得其对角线以下的所有元素相同，而其对角线以上的所有元素也相同.

**问题 3H** 证明，若用三种颜色染 $K_{17}$的边，不管怎样染，必有一个单色三角形.

**问题 3I** 令$\{1, \alpha, \alpha^2, \cdots, \alpha^{14}\}$是$\mathbb{F}_{16}$的乘法群. 用$\mathbb{F}_{16}$里的元素给 $K_{16}$的顶点标号. 我们将用三种颜色染 $K_{16}$的边，使得边$\{i, j\}$染的颜色只依赖于 $\nu$，其中 $\nu$ 满足 $i-j=\alpha^{\nu}$，并能使得 $K_{16}$中没有单色三角形. (按定理 3.3 的表示，这个问题和前一个问题说明了 $N(3, 3, 3; 2)=17$.)

**问题 3J** 对 $K_n$ 的边用红、蓝两种颜色按下述要求进行染色；每条红边最多在一个红色三角形里. 证明存在一个子图 $K_k$ 且 $k\geqslant\lfloor\sqrt{2n}\rfloor$，使得它不含红色三角形.

**问题 3K** 令图 $G$ 满足定理 3.1 的条件. 证明从 $G$ 中最多去掉 $n/d$ 条边后，能找到一个子图 $G'$，它的色数$\leqslant d-1$.

## 评注

在 1976 年以前，四色猜想一直被认为是组合学中最有名的未解决问题之一. Appel 和 Haken 给出的证明引起了许多争论，因为他们的证明很大程度上依赖于计算机对许多情况的分析. 因此证明的有效性依赖于人们对计算机和程序的信赖. (五色定理的两个证明见第 34 章.)

34

布鲁克斯定理，即定理 3.1，是他在剑桥大学上学时发现的，其证明是精妙论证的典型范例，这种证明技巧在图论中常常是必需的，而在这里不使用代数方法.

拉姆齐(F. P. Ramsey, 1902—1928)很年轻时就过世了，以至于他可能有许多结果尚未完成. 他对逻辑系统中的判定方法很感兴趣，并且奇怪地由此引出了这个定理，进而导出了所谓的拉姆齐理论.

定理 3.5 是 P. Erdös(1947)发现的. 关于概率方法的更多内容参阅 Erdös and Spencer (1974).

关于 $N(p, q; 2)$的值和对 $N(p, q; 2)$的估计，请参看 Radziszowski (1999). $N(3, 9; 2)$的值摘自于 Grinstead and Roberts(1982).

定理 3.6 的证明不是 Erdös 和 Szekeres 原来的证明，而他们的证明在通常的书中可以找到. 这里的证明是以色列海法大学的一个学生(M. Tarsy)在一次考试中给出的，他缺席了讲这个定理证明的那次课. 见 Lewin(1976). Johnson(1986)给出了一个类似的证明.

## 参考文献


K. Appel and W. Haken (1977), Every planar map is four-colorable, *Illinois J. Math.* **21**, 429–567.

R. L. Brooks (1941), On colouring the nodes of a network, *Cambridge Philos. Soc.* **37**, 194–197.

P. Erdős (1947), Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.* **53**, 292–294.

P. Erdős and J. L. Spencer (1974), *Probabilistic Methods in Combinatorics*, Academic Press.

P. Erdős and G. Szekeres (1935), A combinatorial problem in geometry, *Compositio Math.* **2**, 463–470.

R. L. Graham and B. L. Rothschild (1974), A short proof of van der Waerden's theorem on arithmetic progressions, *Proc. Amer. Math. Soc.* **42**, 385–386.

R. L. Graham, B. L. Rothschild, and J. L. Spencer (1980), *Ramsey Theory*, Wiley.

C. M. Grinstead and S. M. Roberts (1982), On the Ramsey numbers $R(3,8)$ and $R(3,9)$, *J. Combinatorial Theory* (B) **33**, 27–51.

S. Johnson (1986), A new proof of the Erdős–Szekeres convex $k$-gon result, *J. Combinatorial Theory* (A) **42**, 318–319. [35]

M. Lewin (1976), A new proof of a theorem of Erdős and Szekeres, *The Math. Gazette* **60**, 136–138, 298.

S. P. Radziszowski (1999), Small Ramsey Numbers, *The Electronic Journal of Combinatorics* **1** DS 1.

F. P. Ramsey (1930), On a problem of formal logic, *Proc. London Math. Soc.* (2) **30**, 264–286.

B. L. van der Waerden (1927), Beweis einer Baudetschen Vermutung, *Nieuw Archief voor Wiskunde* **15**, 212–216. [36]

# 第4章　Turán 定理和极图

作为入门，我们先提问一个问题：要保证一个简单图包含三角形，那么这个图至少要有多少条边？因为 $K_{m,m}$ 和 $K_{m,m+1}$ 不含三角形，所以，如果一个图有 $n$ 个顶点，那么 $\lfloor n^2/4 \rfloor$ 条边是不够的. 我们断言，如果它有更多的边，那么这个图就包含三角形(W. Mantel, 1907). 下述证明是令人惊奇的. 设 $G$ 有 $n$ 个顶点，其编号为 1 到 $n$，并且不含三角形. 对每一个顶点 $i$ 给一个权 $z_i \geqslant 0$，使得 $\sum z_i = 1$，并且希望 $S := \sum z_i z_j$ 最大，其中是对所有边 $\{i, j\}$ 求和. 假设顶点 $k$ 和顶点 $l$ 之间没有边，令 $k$ 的邻点的权和为 $x$，而顶点 $l$ 的邻点的权和为 $y$，其中 $x \geqslant y$. 因为 $(z_k+\varepsilon)x+(z_l-\varepsilon)y \geqslant z_k x + z_l y$，所以当把顶点 $l$ 的权之一部分加到顶点 $k$ 的权里，$S$ 的值不会减小. 由此可知，如果所有的权都集中在 $G$ 的某个完全子图上，即一条边的子图上，$S$ 达到最大. 因此，$S \leqslant \frac{1}{4}$. 另一方面，若取所有的 $z_i$ 为 $n^{-1}$，此时 $S$ 的值为 $n^{-2}|E|$. 从而 $|E| \leqslant \frac{1}{4}n^2$.

注意，拉姆齐定理陈述的是：如果一个图有 $n$ 个顶点且 $n \geqslant N(p, q; 2)$，则这个图有 $p$ 个顶点的完全子图，或者存在 $q$ 个顶点且它们之间没边(也称为 $q$ 个顶点的独立集). 我们现在提问这样一个问题：是否对一个图的边数加以限制，就能保证这个图含有 $K_p$ 子图？上面我们已看到，对 $p=3$ 其答案是肯定的. 我们也已有了如何避免 $K_p$ 的思想. 将顶点分为几乎相等大小的 $p-1$ 个子集 $S_1, \cdots, S_{p-1}$，即 $r$ 个含有 $t+1$ 个顶点的子集及 $p-1-r$ 个含有 $t$ 个顶点的子集，其中 $n=t(p-1)+r$，$1 \leqslant r \leqslant p-1$. 每一个 $S_i$ 中没有边，但对 $i \neq j$，$S_i$ 中的每一个顶点与 $S_j$ 中的每一个顶点之间有边连结. (这是一个完全多部图.)这个图的边数为

37

$$M(n,p) := \frac{p-2}{2(p-1)}n^2 - \frac{r(p-1-r)}{2(p-1)}.$$

**定理 4.1**(Turán, 1941)　*如果 $n$ 个顶点的简单图含有多于 $M(n, p)$ 条边时，则它必包含子图 $K_p$.*

**证明**　对 $t$ 进行归纳证明. 当 $t=0$ 时定理显然成立. 设 $G$ 是 $n$ 个顶点的图，不含 $K_p$ 为其子图，并且在满足这些性质的条件下，它的边数最多. 显然 $G$ 包含 $K_{p-1}$(否则增加一条边后仍不含子图 $K_p$)，记 $H$ 是 $G$ 的 $K_{p-1}$ 子图. $G$ 中不在 $H$ 里的每一个顶点，最多与 $H$ 中 $p-2$ 个顶点有边相连. 其余的 $n-p+1$ 个顶点不含子图 $K_p$. 因为 $n-p+1=(t-1)(p-1)+r$，所以可以对这些顶点的集合应用归纳假设. 因此 $G$ 的边数最多为

$$M(n-p+1,p)+(n-p+1)(p-2)+\binom{p-1}{2},$$

且它等于 $M(n, p)$. ■

**注记**　*用于证明芒泰尔(Mantel)定理的论证方法，在这里可以证明，若不存在 $K_p$，那么 $|E| \leqslant \frac{p-2}{2(p-1)}n^2$.*

**问题 4A** $G$ 是 10 个顶点和 26 条边的简单图，证明 $G$ 至少有 5 个三角形. 等式能否出现?

Turán 关于图论的文章包含了定理 4.1，并且他的这篇论文被认为是现在称之为极图理论的起始点——见 Bollobás(1978). 极图问题的一个简单例子是：具有某种性质的一个图最多能有多少条边. 而具有这种性质边数最多的图，称之为*极图*.

Turán 问题的极图只是前面描述的完全多部图. 它是由定理 4.1 的证明过程中的分析而得到的；请读者至少对 $p=3$ 的情况回答下述问题.

38

**问题 4B** 证明 $n$ 个顶点、$\lfloor n^2/4 \rfloor$条边且不含三角形的简单图，如果 $n=2k$，则它是完全二部图 $K_{k,k}$；当 $n=2k+1$ 时，它是 $K_{k,k+1}$.

**问题 4C** 如果 $n$ 个顶点的简单图有 $e$ 条边，那么它至少有$\frac{e}{3n}(4e-n^2)$个三角形.

一个图 $G$ 的*围长*就是 $G$ 中最小多边形 $P_n$ 的边数(一片森林有无限大的围长). 按定义，一个图是简单的，当且仅当它的围长大于等于 3. 根据芒泰尔定理，具有大于 $n^2/4$ 条边的图，它的围长小于等于 3.

**定理 4.2** *如果一个 $n$ 顶点的图 $G$ 有大于$\frac{1}{2}n\sqrt{n-1}$条边，那么 $G$ 的围长小于等于 4. 即 $G$ 不是简单图，或者 $G$ 包含 $P_3$ 或 $P_4$(三角形或 4-边形).*

**证明** 假设 $G$ 的围长大于等于 5. 令 $y_1$，$y_2$，…，$y_d$ 是相邻于顶点 $x$ 的顶点. 其中 $d:=\deg(x)$. 因为 $G$ 不含三角形，所以这些顶点中任何两个不相邻. 进而，因为 $G$ 不含 4-边形，所以除 $x$ 外，任何一个顶点不能与 $y_1$，…，$y_d$ 中两个顶点相邻. 于是$(\deg(y_1)-1)+\cdots+(\deg(y_d)-1)+(d+1)$小于等于 $G$ 的顶点数 $n$. 即有

$$\sum_{y\text{相邻于}x}\deg(y)\leqslant n-1.$$

从而有

$$\begin{aligned}n(n-1)&\geqslant\sum_{x}\sum_{y\text{相邻于}x}\deg(y)=\sum_{y}\deg(y)^2\\&\geqslant\frac{1}{n}\Big(\sum_{y}\deg(y)\Big)^2=\frac{1}{n}(2\mid E(G)\mid)^2.\end{aligned}$$

■

定理 4.2 中的数$\frac{1}{2}n\sqrt{n-1}$是一个界——它不是对所有 $n$ 的精确答案. 对于 $n$ 的一切值，确定这个问题的极图有着不可想象的困难，但是，要确定使等式成立的图已几乎是可能的. 令人惊奇的是，具有 $n>2$ 个顶点、围长$\geqslant 5$，且边数为$\frac{1}{2}n\sqrt{n-1}$的图，最多有 4 个：5-边形($n=5$)，彼得森图($n=10$)，有一个 $n=50$ 的图，可能还有一个 $n=3250$ 的图. 见下面的注记和第 21 章.

39

**问题 4D** 假设 $G$ 是 $r$ 次正则图，围长$\geqslant g$. 求 $\mid V(G)\mid$ 的下界(分别讨论 $g$ 是奇和偶的情形).

一个图有多少条边才能保证它有哈密顿回路(Hamiltonian circuit)不是一个十分有意义的问题，但是一个图的最小次的下界为多少时，才能保证它有哈密顿回路是很有意义的.

**定理 4.3** 如果 $n$ 个顶点的简单图 $G$ 的每一个顶点的次至少为 $n/2$，则它含有一个子图 $P_n$，即有哈密顿回路.

**证明** 假如定理的结论不正确. 令 $G$ 是某 $n$ 个顶点的图且满足定理的假设，但不含哈密顿回路. 我们可以选取具有最多边的这样一个反例，使 $G$ 增加一条边(即两个不相邻顶点间连一条边)后就含有哈密顿回路.

令 $y$ 和 $z$ 是不相邻的顶点. 因为增加边$\{y, z\}$后就有一条哈密顿回路，所以 $G$ 中就有一条从 $y$ 到 $z$ 的简单路，不妨设为 $y=x_1$，$x_2$，…，$x_n=z$. 那么集合

$$\{i: y \text{ 相邻于 } x_{i+1}\}$$

和

$$\{i: z \text{ 相邻于 } x_i\}$$

都至少有 $n/2$ 个元素，并且它们的并集包含在集合$\{1, 2, 3, \cdots, n-1\}$里，因此这两个集合必相交，令 $i_0$ 是它们的一个公共元. 那么

$$y = x_1, x_2, \cdots, x_{i_0}, \quad z = x_n, x_{n-1}, \cdots, x_{i_0+1}, x_1 = y$$

是 $G$ 中长度为 $n$ 的简单闭路的顶点序列，这与作为反例的 $G$ 之选取矛盾. ■

[40] 定理 4.3 归功于狄拉克(G. A. Dirac)，并且在下述意义上是最好可能的：若把 $n/2$ 改为 $(n-1)/2$，则定理就不成立了. 例如，完全二部图 $K_{k,k+1}$没有哈密顿回路，但这个定理的确还可以改进和推广——见 Lovász(1979)，问题 10.21.

**问题 4E** 一块 $3\times3\times3$ 的立方体奶酪被切成 27 块 $1\times1\times1$ 的小立方体. 一只小耗子每天吃一小方块奶酪，相继的两天吃的两小方块奶酪相邻(即两小块奶酪有公共的面). 那么这只小耗子最后一天能否吃到中心那块奶酪?

**问题 4F** 令 $G$ 是 $n$ 个顶点的简单图. 如果 $G$ 的每一个顶点的次大于等于$(n+1)/2$，证明对每一条边 $e$，存在一个哈密顿回路通过 $e$.

**问题 4G** 证明定理 4.1 的注记.

**问题 4H** 证明不含 4 个顶点的回路的图，最多有$\frac{n}{4}(1+\sqrt{4n-3})$条边.

## 评注

P. Turán(1910—1976)是 20 世纪匈牙利著名的数学家之一，他在解析数论以及实分析和复分析方面非常著名.

对每一个 $r\geqslant2$ 和 $g\geqslant2$，存在一个次为 $r$ 的正则图，并且其围长大于等于 $g$. 见 Lovász (1979)，问题 10.12.

分析定理 4.2 的证明，说明具有 $n>2$ 个顶点、围长$\geqslant5$ 及$\frac{1}{2}n\sqrt{n-1}$条边的图，是次为 $k:=\sqrt{n-1}$的正则图，并且这个图中任何一对不相邻的顶点之间有(唯一)一条长度为 2 的路. 若用第 21 章的符号，这样的图就是 $srg(n, k, 0, 1)$，并用第 21 章的方法，说明 $k=2, 3, 7$ 或 57. 这一结果首先出现在 Hoffman and Singleton(1960)中，另外书中还给出了 $k=7$，$n=50$ 的一个例子(这个例子称之为 Hoffman-Singleton 图). 目前我们尚不知是否存在

$srg(3250, 57, 0, 1)$.

## 参考文献

B. Bollobás (1978), *Extremal Graph Theory*, Academic Press.

A. J. Hoffman and R. R. Singleton (1960), On Moore graphs with diameters two and three, *IBM J. Res. Develop.* **4**, 497–504.

[41]

L. Lovász (1979), *Combinatorial Problems and Exercises*, North Holland.

W. Mantel (1907), Problem 28, *Wiskundige Opgaven* **10**, 60–61.

P. Turán (1941), An extremal problem in graph theory (in Hungarian), *Mat. Fiz. Lapok* **48**, 435–452.

[42]

# 第5章　不同代表系

我们首先给出一个定理，称之为霍尔(Hall)婚姻定理的两个不同的表示方式，并给出其一个构造性的证明和一个枚举证明．如果 $A$ 是一个图的顶点子集，用 $\Gamma(A)$ 表示集合 $\bigcup_{a\in A}\Gamma(a)$．讨论顶点集为 $X\cup Y$ 的二部图 $G$(每一边的两个端点，一个在 $X$ 里另一个在 $Y$ 里)．$G$ 中的一个匹配是其边集的一个子集 $E_1$，使得 $G$ 中每一个顶点最多关联于 $E_1$ 中的一条边．从 $X$ 到 $Y$ 的完全匹配，是这样一个匹配，使得 $X$ 中的每一个顶点关联于 $E_1$ 中的一条边．如果 $X$ 和 $Y$ 中的顶点分别被视为男孩和女孩，或者相反情况，而一条边则表示该边两个端点对应的两个人彼此之间有深厚的感情，那么一个完全匹配就表示给 $X$ 中的人指派婚姻配偶的一个可能方案．

**定理 5.1**　*$G$ 中存在从 $X$ 到 $Y$ 的完全匹配的必要和充分条件是，对每一个 $A\subseteq X$，有 $|\Gamma(A)|\geqslant|A|$．*

**证明**　(i)条件的必要性是显然的．

(ii)假定对每一个 $A\subseteq X$，有 $|\Gamma(A)|\geqslant|A|$．令 $|X|=n$，$m<n$，并且假设有一个 $m$ 条边的匹配 $M$．我们将证明存在一个更大的匹配．(这里更大是指基数或者说边的数目，而不是指找出一个包含这 $m$ 条边的完全匹配．)

称匹配 $M$ 中的边为红色边，其余的边为蓝色边．令 $x_0\in X$ 是不关联于匹配中边的一个顶点．我们断定存在从 $x_0$ 出发以蓝色边开始的红蓝边交替出现的一条(奇长)简单路，它终止于蓝色边且终点 $y$ 不关联于匹配中的边．如果找到了这样一条路 $p$，我们从 $M$ 中去掉 $p$ 上的红色边，然后把 $p$ 上的蓝色边加到 $M$ 里，这样就得到一个更大的匹配．换句话说，交换 $p$ 上边的颜色后，红色边的集合为一个更大的匹配．

43

因为 $|\Gamma(\{x_0\})|\geqslant 1$，故存在一个顶点 $y_1$ 相邻于 $x_0$．(由于 $x_0$ 不关联于红色边，显然 $\{x_0, y_1\}$ 是蓝色边．)如果 $y_1$ 也不关联于红色边，我们就得到了所需求的(长度为 1)路；如果 $y_1$ 关联于一条红色边，令 $x_1$ 是这条边的另一个端点．递归地定义 $x_0$，$x_1$，…和 $y_1$，$y_2$，…如下：如果已有 $x_0$，$x_1$，…，$x_k$ 和 $y_1$，$y_2$，…，$y_k$，那么由于 $|\Gamma(\{x_0, x_1, \cdots, x_k\})|\geqslant k+1$，所以存在一个顶点 $y_{k+1}$，它不同于 $y_1$，…，$y_k$，并且它至少与 $\{x_0, x_1, \cdots, x_k\}$ 中一个顶点相邻．如果 $y_{k+1}$ 不关联于红色边，则终止；否则，令 $y_{k+1}$ 关联的红色边的另一个端点为 $x_{k+1}$．

当过程终止时，我们按下述方法构造这条路 $p$：从 $y_{k+1}$ 开始，设与 $y_{k+1}$ 关联的那条蓝色边的另一个端点为 $x_{i_1}$，$i_1<k+1$，然后加上红色边 $\{x_{i_1}, y_{i_1}\}$．按构造过程，$y_{i_1}$ 是以一条(必定是蓝色)边与某个 $x_{i_2}$ 相连，$i_2<i_1$．然后再加红色边 $\{x_{i_2}, y_{i_2}\}$．按这种方式继续下去，直到 $x_0$ 为止．■

**问题 5A**　一个图 $G$($G$ 不必是二部图)的完美匹配，是 $G$ 的这样一个匹配，使得 $G$ 中的每一个顶点都关联于匹配中的一条边．(i)证明有限正则二部图(次为 $d>0$ 的正则)有完美匹配．(ii)构造一个三价(3 次正则)简单图，使其没有完美匹配．(iii)假设 $G$ 是顶点集为 $X\cup Y$ 的二部图(每条边一个端点在 $X$ 中，另一个端点在 $Y$ 里)，并且 $X$ 中每个顶点的次均为 $s>0$，而 $Y$

中每个顶点的次均为 $t$.（这样的条件称为半正则性.）证明，如果 $|X|\leqslant|Y|$（等价地，若 $s\geqslant t$），那么存在自 $X$ 到 $Y$ 的完全匹配 $M$.

**例 5.1** 用一副 52 张的扑克牌做下述游戏：随机地给你 5 张牌．你保留 1 张，把其余的 4 张（按规定的次序）放入一个信封里，然后把它送给你在另一个房间的伙伴．你的伙伴看一下信封里的这些牌，并且说出你保留的那张牌的名字．

应用牌的花色和大小次序值，可能会想出巧妙的或简单的方法去确定保留哪张牌及哪些牌装入信封里，对于你的伙伴而言，确定保留的那张牌是什么，其方法见本章的评注．若不管解的复杂性，对于具有 $N$ 张牌的一副牌而言，其更一般的数学问题为：设 $X$ 为 $N$ 张牌的 $\binom{N}{5}$ 个 5-元子集的集合，$Y$ 为不同牌的 $N(N-1)(N-2)(N-3)$ 个有序 4-元组的集合，那么存在 $X$ 到 $Y$ 的单射 $f$，使得若 $f(S)=(c_1, c_2, c_3, c_4)$，则 $\{c_1, c_2, c_3, c_4\}\subseteq S$.

44

用匹配的术语，我们讨论上述定义的顶点集为 $X\cup Y$ 的二部图 $G$. 其中 $S\in X$ 到 $\{c_1, c_2, c_3, c_4\}\in Y$ 连一边，仅当 $\{c_1, c_2, c_3, c_4\}\subseteq S$. 我们需求 $X$ 到 $Y$ 的一个完全匹配 $M$. 读者可验证，$G$ 是半正则的，并且 $|X|\leqslant|Y|$ 当且仅当 $N\leqslant 124$. 因此由问题 5A(iii)，对 $N\leqslant 124$ 时存在这样一个匹配.

现在我们用集合的术语描述定理 5.1，并且不仅证明这个定理，而且给出其匹配数的下界．设 $A_0, A_1, \cdots, A_{n-1}$ 为有限集 $S$ 的子集．我们说，如果对所有 $k$，$k$ 个子集 $A_i$ 的并有至少 $k$ 个元素，则集合 $\{A_0, A_1, \cdots, A_{n-1}\}$ 有 $H$ 性质（霍尔条件）．如果某 $k$ 个 $A_i$ 的并恰有 $k(0<k<n)$ 个元素，则称这 $k$ 个集合为临界块(block).

集合 $A_0, A_1, \cdots, A_{n-1}$ 的不同代表系(SDR)，定义为 $n$ 个不同元素 $a_0, a_1, \cdots, a_{n-1}$ 的序列，使 $a_i\in A_i$，$0\leqslant i\leqslant n-1$.

令 $m_0\leqslant m_1\leqslant\cdots\leqslant m_{n-1}$，我们定义

$$F_n(m_0, m_1, \cdots, m_{n-1}) := \prod_{i=0}^{n-1}(m_i - i)_*,$$

其中 $(a)_* := \max\{1, a\}$.

从现在起，我们假定序列 $m_i := |A_i|$ 是非减的.

为了证明这个主要定理，我们需要一个引理：

**引理 5.2** 对 $n\geqslant 1$，令 $f_n: \mathbb{Z}^n\to\mathbb{N}$ 定义为

$$f_n(a_0, a_1, \cdots, a_{n-1}) := F_n(m_0, m_1, \cdots, m_{n-1})$$

45

如果 $(m_0, \cdots, m_{n-1})$ 是 $n$-元 $(a_0, \cdots, a_{n-1})$ 的非减重新排列，那么 $f_n$ 关于变量 $a_i$ 中的每一个是非减的.

**证明** 令

$$m_0 \leqslant \cdots \leqslant m_{k-1} \leqslant a_i = m_k \leqslant m_{k+1} \leqslant \cdots \leqslant m_l \leqslant m_{l+1} \leqslant \cdots \leqslant m_{n-1}$$

是 $(a_0, \cdots, a_{n-1})$ 的非减重新排列．如果 $a_i'\geqslant a_i$ 且

$$m_0 \leqslant \cdots \leqslant m_{k-1} \leqslant m_{k+1} \leqslant \cdots \leqslant m_l \leqslant a_i' \leqslant m_{l+1} \leqslant \cdots \leqslant m_{n-1}$$

是 $(a_0, \cdots, a_{i-1}, a_i', a_{i+1}, \cdots, a_{n-1})$ 的非减重新排列，则有

$$\frac{f_n(a_0,\cdots,a_{i-1},a'_i,a_{i+1},\cdots,a_{n-1})}{f_n(a_0,\cdots,a_{n-1})}$$

$$=\frac{(m_{k+1}-k)_*}{(a_i-k)_*}\cdot\frac{(a'_i-l)_*}{(m_l-l)_*}\prod_{j=k+1}^{l-1}\frac{(m_{j+1}-j)_*}{(m_j-j)_*},$$

并且它大于等于1，这是因为对 $j=k+1$，…，$l-1$，有 $a_i\leqslant m_{k+1}$，$a'_i\geqslant m_l$，以及 $m_{j+1}\geqslant m_j$.

■

我们现在讨论霍尔定理的第二种形式. 用 $N(A_0, \cdots, A_{n-1})$ 表示 $(A_0, \cdots, A_{n-1})$ 的不同代表系的个数，即 SDR 的个数.

**定理 5.3** 令 $(A_0, A_{n-1})$ 是集合 $S$ 的子集序列. 令 $m_i := |A_i|$ $(i=0, \cdots, n-1)$，并且 $m_0\leqslant m_1\leqslant\cdots\leqslant m_{n-1}$，若这个序列且有性质 $H$，则

$$N(A_0,\cdots,A_{n-1})\geqslant F_n(m_0,\cdots,m_{n-1}).$$

**证明** 用归纳法证明，显然，对 $n=1$ 定理为真. 我们分两种情况进行讨论.

情况 1. 不存在临界块. 在这种情况下，我们任取 $A_0$ 中的一元素 $a$ 作为其代表，然后从其余的集合中去掉元素 $a$. 这样产生的集合记为 $A_1(a)$，…，$A_{n-1}(a)$. 因无临界块，这些集合具有性质 $H$. 故按归纳假设和引理，我们有

46

$$\begin{aligned}N(A_0,\cdots,A_{n-1})&\geqslant\sum_{a\in A_0}f_{n-1}(|A_1(a)|,\cdots,|A_{n-1}(a)|)\\&\geqslant\sum_{a\in A_0}f_{n-1}(m_1-1,\cdots,m_{n-1}-1)\\&=m_0f_{n-1}(m_1-1,\cdots,m_{n-1}-1)\\&=F_n(m_0,m_1,\cdots,m_{n-1}).\end{aligned}$$

情况 2. 存在临界块 $(A_{v_0}, \cdots, A_{v_{k-1}})$ 且 $v_0<\cdots<v_{k-1}$ 及 $0<k<n$. 在这种情况下，我们从其余的 $A_i$ 中去掉 $A_{v_0}\cup\cdots\cup A_{v_{k-1}}$ 中的所有元素，这样产生的集合记为 $A'_{\mu_0}$，…，$A'_{\mu_{l-1}}$，其中 $\{v_0, \cdots, v_{k-1}, \mu_0, \cdots, \mu_{l-1}\}=\{0, 1, \cdots, n-1\}$，$k+l=n$.

现在 $(A_{v_0}, \cdots, A_{v_{k-1}})$ 和 $(A'_{\mu_0}, \cdots, A'_{\mu_{l-1}})$ 都具有性质 $H$，并且这两个序列的不同代表系是不相交的. 因此，按归纳假设和引理，我们有

$$\begin{aligned}N(A_0,\cdots,A_{n-1})&=N(A_{v_0},\cdots,A_{v_{k-1}})N(A'_{\mu_0},\cdots,A'_{\mu_{l-1}})\\&\geqslant f_k(m_{v_0},\cdots,m_{v_{k-1}})f_l(|A'_{\mu_0}|,\cdots,|A'_{u_{l-1}}|)\\&\geqslant f_k(m_{v_0},\cdots,m_{v_{k-1}})f_l(m_{\mu_0}-k,\cdots,m_{\mu_{l-1}}-k)\\&\geqslant f_k(m_0,\cdots,m_{k-1})f_l(m_{\mu_0}-k,\cdots,m_{\mu_{l-1}}-k).\end{aligned}\tag{5.1}$$

注意

$$m_{v_{k-1}}\leqslant|A_{v_0}\cup\cdots\cup A_{v_{k-1}}|=k,$$

因此我们有

$$(m_r-r)_*=1\qquad 若\quad k\leqslant r\leqslant v_{k-1},$$

及

$$(m_{\mu_i}-k-i)_*=1,\quad 若\quad \mu_i\leqslant v_{k-1}.$$

由此推出

$$f_k(m_0,\cdots,m_{k-1}) = \prod_{0\leqslant i\leqslant v_{k-1}} (m_i - i)_*,$$

$$f_l(m_{\mu_0}-k,\cdots,m_{\mu_{l-1}}-k) = \prod_{v_{k-1}<j<n} (m_j - j)_*,$$

47

也就是说，式(5.1)中最后两项相乘等于 $F_n(m_0, \cdots, m_{n-1})$. 定理证毕. ■

**问题 5B** 定理 5.3 给出了仅与诸 $|A_i|$ 大小有关的诸集合 $A_i$ 的不同代表系个数的下界. 证明这个下界是最好的.

我们现在讨论一个定理，称之为柯尼希(König)定理. 它等价于霍尔定理. 在这个定理中，$A$ 是一个(0, 1)-矩阵，其元素用 $a_{ij}$ 表示. 我们把 $A$ 的行和列都称为线.

**定理 5.4** *覆盖 $A$ 中所有 1 的线之最小条数，等于 $A$ 中不在同一线上 1 的最大个数.*

**证明** 令覆盖 $A$ 中所有 1 的线之最小条数为 $m$，$A$ 中不在同一线上 1 的最大个数为 $M$. 显然有 $m\geqslant M$. 令覆盖 $A$ 中所有 1 的这 $m$ 条线，是由 $r$ 行和 $s$ 列组成(即，$r+s=m$). 不失一般性，设它们是头 $r$ 行和头 $s$ 列. 我们现在定义集合 $A_i$，$1\leqslant i\leqslant r$；$A_i := \{j>s : a_{ij}=1\}$. 如果有某 $k$ 个 $A_i$ 的并含小于 $k$ 个元素，则可以用 $k-1$ 列替换相应的这 $k$ 行，这样仍能覆盖所有的 1. 因为这是不可能的(否则，与线的最小条数矛盾)，所以诸 $A_i$ 满足性质 $H$. 因此，诸 $A_i$ 有 SDR. 这就意味着，在头 $r$ 行而不在头 $s$ 列里存在 $r$ 个 1，使它们其中任何两个不在同一线上. 同样可证，在头 $s$ 列而不在头 $r$ 行里存在 $s$ 个 1，使它们其中任何两个不在同一线上. 这就推出 $M\geqslant r+s=m$. 证毕. ■

下述的伯克霍夫定理是霍尔定理的一个应用.

**定理 5.5** *设 $A=(a_{ij})$ 是一个 $n\times n$ 的非负整数矩阵，使得 $A$ 的每行和每列的和均为 $l$. 则 $A$ 是 $l$ 个置换矩阵的和.*

**证明** 定义 $A_i := \{j : a_{ij}>0\}$，$1\leqslant i\leqslant n$. 对任意的 $k$ 个 $A_i$ 组成的 $k$-元有序组($k$-tuple)，对应 $A$ 的行之和是 $kl$. 因为 $A$ 的每一列之和为 $l$，所以在已选取的这 $k$ 行里的非零元素至少在 $k$ 列里. 因此诸 $A_i$ 满足性质 $H$. 诸 $A_i$ 的一个 SDR 对应于一个置换矩阵 $P=(p_{ij})$，使得若 $p_{ij}=1$，则 $a_{ij}>0$. 从而对 $l$ 使用归纳法即定理得证. ■

48

**问题 5C** 在定理 5.5 中，把整数的假设改为实数，在这种情况下证明 $A$ 是置换矩阵的非负线性组合.（等价地，每一个双随机矩阵(见第 11 章)，是置换矩阵的凸组合.）

**问题 5D** 令集合 $S := \{1, 2, \cdots, mn\}$. 把集合 $S$ 划分为规模为 $n$ 的 $m$ 个集合 $A_1$，$A_2$，$\cdots$，$A_m$. 而且 $B_1$，$B_2$，$\cdots$，$B_m$ 也是 $S$ 的一个划分，其中每一个 $B_i$ 的规模也是 $n$. 证明诸集合 $A_i$ 可以重新编号，使得 $A_i\cap B_i\neq\varnothing$.

**问题 5E** 令 $A_i=\{i-1, i, i+1\}\cap\{1, 2, \cdots, n\}$，$i=1, 2, \cdots, n$，用 $S_n$ 表示集合 $\{A_1, \cdots, A_n\}$的 SDR 的数目，确定 $S_n$ 和 $\lim\limits_{n\to\infty} S_n^{1/n}$ 之值.

设 $G$ 是有限或无限的二部图；它的顶点集划分为 $X$ 和 $Y$，使 $G$ 的每一条边的两个端点分属于 $X$ 和 $Y$. 我们称 $G$ 的一个匹配 $M$ *覆盖*顶点子集 $S$，如果 $S$ 中的每一个顶点都关联于 $M$ 中的一条边.

**定理 5.6** *如果二部图 $G$ 存在一个匹配 $M_1$ 覆盖 $X$ 的一个子集 $X_0$，并且也存在一个匹配 $M_2$ 覆盖 $Y$ 的一个子集 $Y_0$，则 $G$ 有一个匹配 $M_3$，它覆盖顶点集 $X_0\cup Y_0$.*

**证明** 把 $M_1$ 中的边视为红边，$M_2$ 中的边视为蓝边．如果一边既在 $M_1$ 里又在 $M_2$ 里，则视为紫边．

容易看出，每一个顶点的次最多为 2 的连通图是下述图之一：有限的路-图（当分支有一个顶点且没有边时，是属于长度为 0 的情况）；有限多边形；无限的单侧路-图（具有一个一价顶点）；无限的双侧路-图．由 $G$ 的顶点集以及匹配 $M_1$ 和 $M_2$ 的边集 $M_1 \cup M_2$ 构成的图记为 $H$，则 $H$ 的每一个顶点的次最多为 2，因此 $H$ 的连通分支是属于上述列出的类型．除包含紫边及紫边的端点的图外，任一个分支中的边是红蓝交替的．特别地，所有多边形都是偶长的．$X_0 \cup Y_0$ 中的每一个顶点都在这些非平凡分支之一里．

49

$M_3$ 可由下述的边组成：所有的紫边及 $H$ 的其他每一个分支中的所有蓝边或红边．对于圈和无限双侧路取所有红边或所有蓝边都可以，它们都能覆盖这个分支的所有顶点．对于奇长的路和无限单侧路而言，取红边还是蓝边，依赖于第一条边是红的还是蓝的（奇长路的第一和最后边的颜色相同，因此不管从哪一端开始都一样）．这样取的边也覆盖了该分支的所有顶点．

对于偶数长的有限路 $P$，我们必须仔细想一下．设这条路的顶点为 $v_0$，$v_1$，…，$v_k$．它有奇数顶点，并且交替地属于 $X$ 和 $Y$，因此 $v_0$ 和 $v_k$ 或都在 $X$ 里，或都在 $Y$ 里．如果它们都在 $X$ 里，那么把 $P$ 上的红边（属于 $M_1$）取出放入 $M_3$；如果它们都在 $Y$ 里，那么把 $P$ 上的蓝边取出放入 $M_3$．这样取出的边，只有路 $P$ 上的一个端点未被覆盖．

只讨论 $v_0$，$v_k \in X$ 的情况（对 $v_0$，$v_k \in Y$ 的情况可完全类似地讨论）．如果 $P$ 的第一条边是红的，那么最后一条边必是蓝的，由于没有 $M_1$ 的边覆盖 $v_k$，所以 $v_k \notin X_0$．因此 $P$ 上的红边仍能覆盖 $X_0$ 和 $Y_0$ 在 $P$ 上的所有顶点．类似地，若 $P$ 的第一条边是蓝色，则 $v_0 \notin X_0$，并且 $P$ 的所有红边仍覆盖了 $X_0$ 和 $Y_0$ 在 $P$ 上的所有顶点． ■

对 $X_0 = X$，$Y_0 = Y$ 的情形，当 $G$ 是完全二部图时，覆盖 $X_0$ 或 $Y_0$ 的匹配分别对应于或解释为 $X \to Y$ 的单射或 $Y \to X$ 的单射．定理 5.6 表明：

**推论** *设 $X$ 和 $Y$ 是两个集合，若存在单射 $f: X \to Y$ 和 $g: Y \to X$，则存在从 $X$ 到 $Y$ 或 $Y$ 到 $X$ 的双射，即这两个集合之间存在 1-1 对应．*

50

用集合的基数术语表示：如果 $|X| \leqslant |Y|$ 且 $|Y| \leqslant |X|$，则 $|X| = |Y|$．这就是施罗德-伯恩斯坦（Schröder-Bernstein）定理；参看 P. R. Halmos(1974)的第 22 节．当然，对有限集这是显然的．

**问题 5F** 令 $A_1$，$A_2$，…，$A_n$ 是有限集．证明：如果

$$\sum_{1 \leqslant i < j \leqslant n} \frac{|A_i \cap A_j|}{|A_i| \cdot |A_j|} < 1,$$

则集合 $A_1$，$A_2$，…，$A_n$ 有不同代表系．

**问题 5G** (i)由问题 5A，我们知道具有 $2n$ 个顶点的 3 次正则二部图有完美匹配．如果 $n=4$，它有多少个不同的完美匹配呢？(ii)对于 10 个顶点次为 4 的正则二部图，有多少个不同的完美匹配？

**评注**

霍尔（Philip Hall）的结果是在 1935 年发表的（其证明相当困难）．这里给出的证明是

Halmos 和 Vaughan、Rado 及 M. Hall 思想的推广. 这个证明归功于 Ostrand(1970)以及 Hautus and van Lint(1972). 参见 van Lint(1974). 完全匹配问题，通常称为婚姻问题(marriage problem).

D. König(1884—1944)是布达佩斯(Budapest)的一位教授. 他首次对图论进行了广泛的论述(Theorie der endlichen und unendlichen Graphen, 1936). König(1916)给出了一个定理(称之为柯尼希定理)的第一个证明.

在定理 5.4 的上面一段里，我们提出了这些定理的"等价性". 当两个定理中的一个近乎是另一个的直接结果时，通常就说它们是等价的.

Birkhoff(1946)给出的定理，即定理 5.5 是非常有用的，在后面的几章里将多次被使用.

对例 5.1 中的扑克牌问题，现在给出一种求解方法. 在 5 张牌一组里，某一种花色必出现至少两次. 给你伙伴的第一张牌应该是两张花色相同中的"较大"者，而你保留的是二者中的"较小"者，这里我们把次序 2，3，…，10，J，Q，K，A，顺时针排列成一个圈(mod 13)；二者中的"较小"者是指从它开始，按顺时针方向通过最短的距离到达另一个. 例如，若 $S=\{3\spadesuit, Q\diamondsuit, 6\clubsuit, 3\diamondsuit, 7\spadesuit\}$，那么你把 $7\spadesuit$ 或 $3\diamondsuit$ 给你的伙伴. 这就等于已告诉了你的伙伴你保留的那张牌的花色，以及你保留的那张牌仅有 6 种可能性. 为了确定从第一张牌出发(逆时针)返回到"较小"那张牌的距离，你和你的伙伴要用剩余的 3 张牌的顺序(52 张牌可按字典序排列)，约定 3 个对象的 6 个排列与整数 1，2，…，6 之间的对应性. [51]

## 参考文献


G. Birkhoff (1946), Tres observaciones sobre el algebra lineal, *Univ. Nac. Tucumán, Rev.* Ser. A, **5**, 147–151.

P. Hall (1935), On representatives of subsets, *J. London Math. Soc.* **10**, 26–30.

P. R. Halmos (1974), Naive Set Theory, Springer-Verlag.

D. König (1916), Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre, *Math. Annalen* **77**, 453–465.

J. H. van Lint (1974), *Combinatorial Theory Seminar Eindhoven University of Technology*, Lecture Notes in Mathematics **382**, Springer-Verlag.

P. Ostrand (1970), Systems of distinct representatives, *J. of Math. Analysis and Applic.* **32**, 1–4.

[52]

# 第6章　迪尔沃斯定理和极集理论

一个偏序集(简记为poset)就是一个集合 $S$ 连同 $S$ 上的一个二元关系 $\leqslant$(有时用 $\subseteq$)，使其满足：

(i)对一切 $a\in S$ 有 $a\leqslant a$(反射性).

(ii)若 $a\leqslant b$，$b\leqslant c$，则 $a\leqslant c$(传递性).

(iii)若 $a\leqslant b$ 且 $b\leqslant a$，则 $a=b$(反对称性).

如果对 $S$ 中任意两个元素 $a$ 和 $b$，或者 $a\leqslant b$ 或者 $b\leqslant a$，则这个偏序称为*全序*或*线性序*. 如果 $a\leqslant b$ 且 $a\neq b$，那么记为 $a<b$. 例如，整数集及整数间的通常的大小关系就构成一个偏序集；一个集的子集及集合的包含关系也构成一个偏序集. 如果集合 $S$ 的一个子集是全序的，那么这个子集就称为是一条*链*. 若一个集合中的元素是两两不可比较的，则这个集合称为*反链*.

下述定理归功于R. Dilworth(1950)，下述的证明是H. Tverberg(1967)给出的.

**定理6.1**　*令 $P$ 是一个有限偏序集. $P$ 中元素划分为不相交链的最小个数 $m$，等于 $P$ 的一个反链所含元素的最大个数 $M$.*

**证明**　(i)显然有 $m\geqslant M$.

(ii)对 $|P|$ 使用归纳法. 若 $|P|=0$，显然定理为真. 令 $C$ 是 $P$ 的一条极大链. 如果 $P\setminus C$中每一个反链包含最多 $M-1$ 个元素，则定理成立. 因此，假设 $\{a_1, a_2, \cdots, a_M\}$ 是 $P\setminus C$ 中的一个反链. 我们定义 $S^-:=\{x\in P:\exists_i[x\leqslant a_i]\}$，类似地定义 $S^+$. 因为 $C$ 是极大链，所以 $C$ 中的最大元不在 $S^-$ 里，故按归纳假设，对 $S^-$ 定理成立. 因此 $S^-$ 是 $M$ 个不交的链 $S_1^-$，$S_2^-$，…，$S_M^-$ 的并，其中 $a_i\in S_i^-$. 假设 $x\in S_i^-$ 且 $x>a_i$. 因为存在 $j$，使 $x\leqslant a_j$，从而有 $a_i<a_j$，这与 $\{a_1, a_2, \cdots, a_M\}$ 是反链矛盾. 这样就证明了 $a_i$ 是 $S_i^-$ 的极大元，其中 $i=1, 2, \cdots, M$[⊖]. 我们可同样地对 $S^+$ 进行讨论. 与链联系起来，这个定理就得到了证明. ■



Mirsky(1971)给出了迪尔沃斯(Dilworth)定理的对偶.

**定理6.2**　*令 $P$ 是一个偏序集. 如果 $P$ 不具有 $m+1$ 个元素的链，则 $P$ 是 $m$ 个反链的并.*

**证明**　对 $m=1$，定理显然成立. 令 $m\geqslant 2$ 且假定对 $m-1$ 定理为真. 令 $P$ 是一个偏序集且没有 $m+1$ 个元素的链. 令 $M$ 是 $P$ 的极大元集合，则 $M$ 是一个反链. 假设 $x_1<x_2<\cdots<x_m$ 是 $P\setminus M$ 中的一条链，那么它也是 $P$ 的极大链，因此 $x_m\in M$，故得矛盾. 所以 $P\setminus M$ 没有 $m$ 个元素的链. 故按归纳假设，$P\setminus M$ 是 $m-1$ 个反链的并. 定理得证. ■

下述的著名定理归功于Sperner(1928)，它与上述定理有相似的性质，这个定理的下述证明是Lubell(1966)给出的.

**定理6.3**　*如果 $A_1$，$A_2$，…，$A_m$ 是 $N:=\{1, 2, \cdots, n\}$ 的一些子集，且满足对任意 $i\neq j$，$A_i$ 不是 $A_j$ 的子集，那么 $m\leqslant\binom{n}{\lfloor n/2\rfloor}$.*

---

⊖ 这里原文为 $m$，与上下文不合. ——译者注

**证明** 考虑由 $N$ 的子集构成的偏序集. $\mathcal{A}:=\{A_1, A_2, \cdots, A_m\}$是这个偏序集的一个反链.

这个偏序集的一个极大链$\mathcal{C}$由元素个数为 $i$ 的子集组成，其中 $i=0, 1, \cdots, n$，它可按下述方法得到：开始的一个是空集，然后是包含一个单一元素的子集(有 $n$ 种选取)，接下来是包含前面子集的 2-子集(有 $n-1$ 种选取)，再接下来是包含前面子集的 3-子集(有 $n-2$ 种选取)，如此等等. 因此有 $n!$ 个极大链. 类似地，给定 $N$ 的一个 $k$-子集 $A$，恰有 $k!\,(n-k)!$ 个极大链包含 $A$.

现在计算有序对$(A, \mathcal{C})$的个数，其中 $A\in\mathcal{A}$，$\mathcal{C}$是极大链，而 $A\in\mathcal{C}$. 因为每一个极大链$\mathcal{C}$最多包含一个反链中的一个成员，因此有序对的个数最多为 $n!$ 个. 若令 $A\in\mathcal{A}$且 $|A|=k$ 的子集的个数为 $\alpha_k$，那么有序对的个数为 $\sum_{k=0}^{n}\alpha_k k!(n-k)!$. 因此

$$\sum_{k=0}^{n}\alpha_k k!(n-k)! \leqslant n! \quad \text{或等价于} \quad \sum_{k=0}^{n}\frac{\alpha_k}{\binom{n}{k}} \leqslant 1.$$

54

因为 $k=\lfloor n/2\rfloor$时，$\binom{n}{k}$达到最大，以及 $\sum\alpha_k=m$，由此可得到定理的结论. ■

如果我们取 $N$ 的所有$\lfloor n/2\rfloor$-子集作为反链，则定理 6.3 中的等式成立.

现在我们讨论由 $n$-集 $N$ 的所有子集($2^n$ 个)在集合包含关系下组成的偏序集 $B_n$. $N$ 的 $i$-子集的集合用$\mathcal{A}_i$ 表示. $B_n$ 的一条对称链定义为顶点的一个序列 $P_k, P_{k+1}, \cdots, P_{n-k}$，使得对 $i=k, k+1, \cdots, n-k-1$ 有 $P_i\in\mathcal{A}_i$ 和 $P_i\subseteq P_{i+1}$. 现在我们叙述由 De Bruijn, Van Ebbenhorst Tengbergen and Kruyswijk(1949)给出的把 $B_n$ 分裂为(不相交)对称链的算法.

**算法**：从 $B_1$ 开始，归纳地进行. 如果 $B_n$ 已被分裂为对称链，那么对每一个这样的对称链 $P_k, \cdots, P_{n-k}$，定义 $B_{n+1}$中的两个对称链，即 $P_{k+1}, \cdots, P_{n-k}$和 $P_k, P_k\cup\{n+1\}, P_{k+1}\cup\{n+1\}, \cdots, P_{n-k}\cup\{n+1\}$.

容易看出，这个算法确实把 $B_n$ 分裂为对称链，进而还提供了 $B_n$ 的 $k$-子集和$(n-k)$-子集之间的一个自然的匹配(参看定理 5.1). 也可见下述问题 6D.

**问题 6A** 令 $a_1, a_2, \cdots, a_{n^2+1}$是整数 $1, 2, \cdots, n^2+1$ 的一个置换. 证明由迪尔沃斯定理可推出，这个序列中有一个长为 $n+1$ 的单调子序列.

下述是问题 6A 的一个优美的直接证明. 假设不存在 $n+1$ 项的递增子序列. 令 $b_i$ 是自 $a_i$ 项开始的最长递增子序列的长度. 那么按鸽巢原理，在这些 $b_i$-序列里至少有 $n+1$ 个有相同的长度. 因为 $i<j$ 且 $b_i=b_j$，则必有 $a_i>a_j$，因此我们就得到长为 $n+1$ 的递减子序列.

为了说明第 5 章和第 6 章之间的联系，我们现在证明定理 5.1 可由定理 6.1 直接推出. 考虑定理 5.1 中的二部图 $G$. 令 $|X|=n$，$|Y|=n'\geqslant n$. 我们引进一个偏序集：定义 $x_i<y_i$ 当且仅当从顶点 $x_i$ 到顶点 $y_i$ 有边. 假定最大反链有 $s$ 个元素，设这个反链为$\{x_1, x_2, \cdots, x_h, y_1, \cdots, y_k\}$，其中 $h+k=s$. 因为 $\Gamma(\{x_1, \cdots, x_h\})\subseteq Y\setminus\{y_1, \cdots, y_k\}$，从而 $h\leqslant n'-k$. 因此 $s\leqslant n'$. 这个偏序集是 $s$ 个不交的链的并. 这 $s$ 个不交的链由大小为 $a$ 的一个匹配 $X$ 中 $n-a$ 个元素和 $Y$ 中 $n'-a$ 个元素组成. 因此 $n+n'-a=s\leqslant n'$，即 $a\geqslant n$，这就意味着有一个完全匹配.

55

定理 6.3 是通常称之为极集理论领域里的一个相当容易的例子，而极集理论中的问题通常是十分困难的．下面我们再给出一个例子作为简单练习．

**问题 6B** 令 $A_i(1\leqslant i\leqslant k)$ 是集合 $\{1, 2, \cdots, n\}$ 的 $k$ 个不同的子集．假设对所有的 $i$ 和 $j$ 有 $A_i\cap A_j\neq\varnothing$，证明 $k\leqslant 2^{n-1}$，并给出使等式成立的一个例子．

我们再介绍一个典型的方法，该方法在证明 Sperner 定理时使用过．我们证明埃德斯-柯召-拉多(Erdös-Ko-Rado)定理(1961)．

**定理 6.4** 令 $\mathcal{A}=\{A_1, \cdots, A_m\}$ 是集合 $\{1, 2, \cdots, n\}$ 的 $m$ 个不同 $k$-子集的集合，使得任何两个子集有非空的交，其中 $k\leqslant n/2$．证明 $m\leqslant\binom{n-1}{k-1}$．

**证明** 将 1 到 $n$ 这 $n$ 个整数由小到大排成一个圆圈，令 $F_i$ 表示集合 $\{i, i+1, \cdots, i+k-1\}$，其中这些整数取模 $n$．记 $\mathcal{F}:=\{F_1, F_2, \cdots, F_n\}$ 为圈上所有 $k$ 个相继元素集合的总体．由于如果某个 $F_i$ 等于某个 $A_j$，那么集合 $\{l, l+1, \cdots, l+k-1\}$ 和 $\{l-k, \cdots, l-1\}(i<l<i+k)$ 中最多有一个在 $\mathcal{A}$ 中，所以 $|\mathcal{A}\cap\mathcal{F}|\leqslant k$．对 $\{1, 2, \cdots, n\}$ 应用一个置换 $\pi$，则由 $\mathcal{F}$ 得到 $\mathcal{F}^\pi$，那么对 $\mathcal{F}^\pi$ 上述结论同样成立．因此有

$$\Sigma:=\sum_{\pi\in S_n}|\mathcal{A}\cap\mathcal{F}^\pi|\leqslant k\cdot n!.$$

我们固定 $A_j\in\mathcal{A}$ 和 $F_i\in\mathcal{F}$，计算这个和，并注意到使 $F_i^\pi=A_j$ 的置换有 $k!(n-k)!$ 个．因此 $\Sigma=m\cdot n\cdot k!(n-k)!$．这样定理就得到了证明． ■

如果假定 $\mathcal{A}$ 中每一个集合最多含有 $k$ 个元素，并且它们构成一条反链，那么对上述证明略加修改，就能证明在这种条件下该定理仍然成立．但是我们将用定理 5.1 给予证明．

56

**定理 6.5** 令 $\mathcal{A}=\{A_1, \cdots, A_m\}$ 是集合 $N:=\{1, 2, \cdots, n\}$ 的 $m$ 个子集的集合，使得对 $i\neq j$ 有 $A_i\not\subseteq A_j$ 且 $A_i\cap A_j\neq\varnothing$ 以及对一切 $i$ 有 $|A_i|\leqslant k\leqslant n/2$，则 $m\leqslant\binom{n-1}{k-1}$．

**证明** (i)如果所有子集都有 $k$ 个元素，则按定理 6.4 结论成立．

(ii)令 $A_1, \cdots, A_s$ 是基数最小的子集，设其基数为 $l\leqslant\frac{n}{2}-1$．考虑 $N$ 的包含一个或多个 $A_i(1\leqslant i\leqslant s)$ 的所有 $(l+1)$-子集 $B_j$．显然这些 $B_j$ 均不在 $\mathcal{A}$ 里．每一个集合 $A_i(1\leqslant i\leqslant s)$ 恰在 $n-l$ 个 $B_j$ 里，并且每一个 $B_j$ 最多包含 $l+1\leqslant n-l$ 个 $A_i$．因此，按定理 5.1，可以选取 $s$ 个不同的集合，比如 $B_1, \cdots, B_s$，使得 $A_i\subseteq B_i$．如果用 $B_i$ 替换 $A_i$，那么新的集合 $\mathcal{A}'$ 满足定理的条件，且最小基数的子集有大于 $l$ 个元素．按归纳法，可归结为情况(i)． ■

把定理 6.4 证明中的计数论证改为赋权子集的计数论证，这样，我们就能证明下述推广，它属于 B. Bollobás(1973)．

**定理 6.6** 令 $\mathcal{A}=\{A_1, \cdots, A_m\}$ 是 $\{1, 2, \cdots, n\}$ 的 $m$ 个不同子集的集合，其中对 $i=1, \cdots, m$，有 $|A_i|\leqslant n/2$．如果任何两个子集都有非空的交，则

$$\sum_{i=1}^{m}\frac{1}{\binom{n-1}{|A_i|-1}}\leqslant 1.$$

**证明** 设 $\pi$ 是排成一个圈的 1，2，…，$n$ 的一个置换，如果 $A_i$ 中的元素相继地出现在该圈的某一段，则称 $A_i \in \pi$. 与定理 6.4 的证明相同，我们可证，若 $A_i \in \pi$，则所有满足 $A_j \in \pi$ 的 $j$ 最多有 $|A_i|$ 个.

定义

$$f(\pi,i) := \begin{cases} \dfrac{1}{|A_i|}, & 若\ A_i \in \pi \\ 0, & 其他. \end{cases}$$

根据上述论证 $\sum_{\pi \in S_n} \sum_{i=1}^{m} f(\pi,i) \leqslant n!$. 改变和的次序，对于固定的 $A_i$，我们必须计算置换 $\pi$ 排成一个圈使 $A_i \in \pi$ 的 $\pi$ 的个数. 这个数(用定理 6.4 的相同论证)是 $n \cdot |A_i|!\ (n-|A_i|)!$. 因此有 57

$$\sum_{i=1}^{m} \frac{1}{|A_i|} \cdot n \cdot |A_i|!(n-|A_i|)! \leqslant n!,$$

由此可得所需结果. ■

**问题 6C** 令 $\mathcal{A}=\{A_1, \cdots, A_m\}$ 是 $N := \{1, 2, \cdots, n\}$ 的 $m$ 个不同的子集的集合，使得若 $i \neq j$，则 $A_i \not\subseteq A_j$，$A_i \cap A_j \neq \varnothing$，$A_i \cup A_j \neq N$. 证明

$$m \leqslant \binom{n-1}{\left\lfloor \frac{n}{2} \right\rfloor - 1}.$$

**问题 6D** 考虑把 $B_n$ 按上述描述分解为对称链. 证明定理 6.3 是这种分解的一个直接结果. 证明定理 6.5 通过这种分解能归结为定理 6.4. 使链的最小元在 $\mathcal{A}_i$ 里的链有多少个?

**问题 6E** 给定偏序集 $B_n$ 的一个元素 $S$($\{1, 2, \cdots, n\}$的一个子集)，构造 $B_n$ 包含 $S$ 的对称链的算法. 用 $x$ 表示 $S$ 的特征向量；例如 $n=7$，$S=\{3, 4, 7\}$，那么 $x=0011001$. 标记所有相继的 10 对，暂时去掉这些标记的对，然后再标记所有相继的 10 对，重复这个过程，一直到剩下的数串为形式 $00\cdots01\cdots11$ 为止. 在我们的例子里，我们得到 $00\dot{1}\dot{1}\dot{0}\dot{0}1$，其中对 $i=3$，4，5，6，第 $i$ 个坐标被标记，当去掉这些被标记的坐标后，剩余数串为 001. 这条链上的诸子集的特征向量可如下得到：固定所有被标记的坐标，然后让其余坐标组成的数串取遍 $0\cdots000$，$0\cdots001$，$0\cdots011$，…，$1\cdots111$. 在我们的例子里，这些特征向量为

$$00\dot{1}\dot{1}\dot{0}\dot{0}0,$$

$$00\dot{1}\dot{1}\dot{0}\dot{0}1,$$

$$01\dot{1}\dot{1}\dot{0}\dot{0}1,$$

$$11\dot{1}\dot{1}\dot{0}\dot{0}1,$$ 58

它们对应的子集为

$$\{3,4\},\{3,4,7\},\{2,3,4,7\},\{1,2,3,4,7\}.$$

证明这个算法生成的包含 $S$ 的对称链，与下述德布鲁因等归纳算法所得到的对称链恰好相同.

## 评注

我们将在第 23 章和第 25 章转到偏序集.

E. Sperner(1905—1980)是以组合拓扑学中的一个引理而出名的，通常把这个引理称之为"Sperner 引理". 该引理出现在他的毕业论文里(1928)，被用于证明布劳威尔(Brouwer)的不动点定理.（与组合学的另一个联系是他最先在哥尼斯堡大学取得教授资格!）他是著名的Oberwolfach 研究所的创始人之一.

关于极集理论的综述，请参看 Frankl(1988).

Katona(1974)给出了埃德斯-柯召-拉多定理的一个简短的证明. 定理 6.5 归功于 Kleitman and Spencer(1973)以及 Schönheim(1971). 定理 6.6 的证明是由 Greene, Katona and Kleitman(1976)给出的.

## 参考文献


B. Bollobás (1973), Sperner systems consisting of pairs of complementary subsets, *J. Combinatorial Theory* (A) **15**, 363–366.

N. G. de Bruijn, C. van Ebbenhorst Tengbergen and D. Kruyswijk (1949), On the set of divisors of a number, *Nieuw Archief v. Wisk.* (2) **23**, 191–193.

R. P. Dilworth (1950), A decomposition theorem for partially ordered sets, *Annals of Math.* (2) **51**, 161–166.

P. Erdős, Chao Ko, and R. Rado (1961), Extremal problems among subsets of a set, *Quart. J. Math. Oxford* Ser. (2) **12**, 313–318.

P. Frankl (1988), Old and new problems on finite sets, Proc. Nineteenth S. E. Conf. on Combinatorics, Graph Th. and Computing, Baton Rouge, 1988.

C. Greene, G. Katona, and D. J. Kleitman (1976), Extensions of the Erdős–Ko–Rado theorem, *Stud. Appl. Math.* **55**, 1–8.

59

G. O. H. Katona (1974), Extremal problems for hypergraphs, in *Combinatorics* (edited by M. Hall, Jr. and J. H. van Lint), Reidel.

D. J. Kleitman and J. Spencer (1973), Families of $k$-independent sets, *Discrete Math.* **6**, 255–262.

D. Lubell (1966), A short proof of Sperner's lemma, *J. Combinatorial Theory* **1**, 299.

L. Mirsky (1971), A dual of Dilworth's decomposition theorem, *Amer. Math. Monthly* **78**, 876–877.

J. Schönheim (1971), A generalization of results of P. Erdős, G. Katona, and D. J. Kleitman concerning Sperner's theorem, *J. Combinatorial Theory* (A) **11**, 111–117.

E. Sperner (1928), Ein Satz über Untermengen einer endlichen Menge, *Math. Zeitschrift* **27**, 544–548.

H. Tverberg (1967), On Dilworth's decomposition theorem for partially ordered sets, *J. Combinatorial Theory* **3**, 305–306.

60

# 第7章 网 络 流

一个运输网络，就是一个有限的有向图 $D$ 连同两个特殊的顶点 $s$ 和 $t$（分别称为发点和收点），以及每一边 $e$ 上有一个非负的实数 $c(e)$（称为边 $e$ 的容量）．我们假定运输网络中没有环和多重边，并且没有进入发点 $s$ 的边，也没有离开收点 $t$ 的边（虽然有这些类型的边也无妨碍，但在定义上需要更详细）．

我们给出图 7.1 中的一个例子．设想一下管道网络，某种流体沿着箭头的方向通过这个网络．一条边上的容量表示沿着这段管道的（单位时间）最大可能的流量．

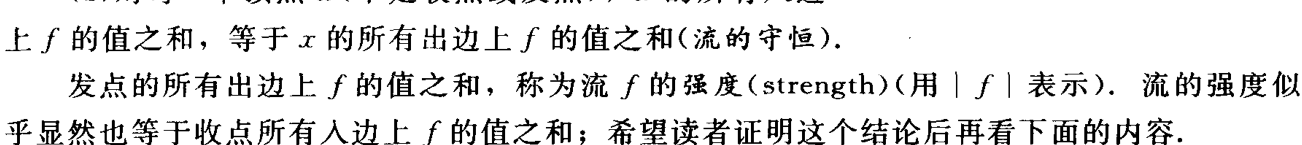
图 7.1

61

运输网络中的一个流(flow)是边集上的一个函数 $f$，它对每一边 $e$ 给出一个实数 $f(e)$，使其满足：

(a) $0\leqslant f(e)\leqslant c(e)$ 对一切边 $e$ 成立（流是可行的）．

(b) 对每一个顶点 $x$（不是收点或发点），$x$ 的所有入边上 $f$ 的值之和，等于 $x$ 的所有出边上 $f$ 的值之和（流的守恒）．



发点的所有出边上 $f$ 的值之和，称为流 $f$ 的强度(strength)（用 $|f|$ 表示）．流的强度似乎显然也等于收点所有入边上 $f$ 的值之和；希望读者证明这个结论后再看下面的内容．

我们的目标之一是找出构造最大流，即具有最大强度的流的一种方法．首先，若有一个目标或者流的强度的上界，那将是有益的；例如，自发点出去的所有边的容量和，显然是这样一个上界．更一般地，分离 $s$ 和 $t$ 的割（或简称为割），是指顶点集 $V:=V(D)$ 的一个划分 $(X, Y)$，使 $s\in X$，$t\in Y$．定义这个割的容量为 $c(X, Y)$，它是从 $X$ 到 $Y$ 的所有边的容量之和（即这些边 $e:=(x, y)$，$x\in X$，$y\in Y$）．我们断定任一个割的容量是任一个流的强度之上界．更强的结果是，我们断言由流的守恒定律可推出（见后续）一个流 $f$ 的强度可用下式计算：

$$|f| = f(X,Y) - f(Y,X), \tag{7.1}$$

其中 $f(A,B)$ 表示从 $A$ 到 $B$ 的所有边上 $f$ 值的总和；那么由 $f$ 的可行性直接推出 $|f|\leqslant c(X,Y)$．因此，一个网络中的所有割的最小容量（例如图 7.1 中，最小割容量为 20），是这个网络中流的强度之上界．

为了建立式(7.1)，我们引进一个函数 $\phi$，对每一顶点 $x$ 和每一条边 $e$，定义 $\phi(x,e)$ 如下：若边 $e$ 为 $x$ 的入边，则 $\phi(x,e):=-1$；若边 $e$ 为 $x$ 的出边，则 $\phi(x,e):=+1$；若边 $e$ 与 $x$ 不相关联，那么 $\phi(x,e):=0$．（注意，实质上 $\phi$ 是有向图的关联矩阵，见第 36 章．）守恒定律等价于对一切 $x\neq s,t$，有 $\sum_{e\in E}\phi(x,e)f(e)=0$．注意，如果 $e$ 是自 $X$ 指向 $Y$ 的，则 $\sum_{x\in X}\phi(x,e)=+1$；如果 $e$ 是自 $Y$ 指向 $X$ 的，则 $\sum_{x\in X}\phi(x,e)=-1$；如果 $e$ 的两个端点同时在 $X$ 里或者 $Y$ 里，则 $\sum_{x\in X}\phi(x,e)=0$．因此

62

$$\begin{aligned}|f| &= \sum_{e\in E}\phi(s,e)f(e) = \sum_{x\in X}\sum_{e\in E}\phi(x,e)f(e)\\ &= \sum_{e\in E}f(e)\sum_{x\in X}\phi(x,e) = f(X,Y) - f(Y,X).\end{aligned}$$

(在上述第一个二重和里，对 $x\neq s$ 时其内和为 0.)

对式(7.1)的具体例子有 $|f|=f(V\setminus\{t\},\{t\})$，请读者回顾前面的结论.

现在我们来构造流. 固定一个流 $f$，它可能是 0-流. 不同顶点的一个序列 $x_0, x_1, \cdots, x_{k-1}, x_k$，如果对每一个 $i$，$1\leqslant i\leqslant k$，满足下述条件之一：

(i)$e=(x_{i-1}, x_i)$是一条边且 $c(e)-f(e)>0$，

(ii)$e=(x_i, x_{i-1})$是一条边且 $f(e)>0$，

则称序列 $x_0, x_1, \cdots, x_{k-1}, x_k$ 为自 $x_0$ 到 $x_k$ 的一条*特殊路*. 使 $f(e)=c(e)$的边 $e$ 称为*饱和边*，条件(i)和(ii)可叙述为：关于流 $f$，这条路前向边是非饱和的，而后向边是正的. 假定存在这样一条从 $s$ 到 $t$ 的特殊路，定义 $\alpha_i$ 如下：在情况(i)$\alpha_i=c(e)-f(e)$；在情况(ii)$\alpha_i=f(e)$(如果两种情况均成立，则选取其中一条边). 令 $\alpha$ 是这些正的 $\alpha_i$ 中之最小者. 对情况(i)中每条边上流的值*增加* $\alpha$；对情况(ii)中每条边上流的值*减小* $\alpha$，容易验证，流的两个条件(可行性和守恒)仍满足. 显然新流的强度为 $|f|+\alpha$.

把得到更强流的思想变成一个算法如下：(从 0-流开始)进行迭代，并结合一个系统化的方法搜索关于当前流的从 $s$ 到 $t$ 的特殊路，在本章的评注里，我们对算法的终止进行了简单说明. 然而，当算法不能继续时，将会出现什么情况呢？

假设关于某个流 $f_0$ *不存在从发点到收点的特殊路*，令 $X_0$ 是自 $s$ 出发由特殊路到达的顶点 [63] $x$ 的集合，$Y_0$ 是剩余的顶点集合. 这样我们就得到了一个割. 如果 $x\in X_0$，$y\in Y_0$ 且 $e=(x, y)$是一条边，那么 $e$ 必是饱和边. 否则，我们可以将 $s$ 到 $x$ 的特殊路延长到 $y$，从而得到自 $s$ 到 $y$ 的特殊路. 这与 $X_0$ 和 $Y_0$ 的定义矛盾. 另一方面，若 $e=(y, x)$是一条边，那么类似地可证 $f(e)$必定为 0. 按(7.1)的结果，我们有

$$|f_0|=f_0(X_0,Y_0)-f_0(Y_0,X_0)=c(X_0,Y_0).$$

显然，不仅不可能用特殊路的方法得到更强的流，而且由于对任意流 $f$ 有 $|f|\leqslant c(X_0, Y_0)$，所以根本不可能存在更强的流.

如果选取 $f_0$ 是一个最大流(在算法终止不能肯定的情况下，根据连续性的理由，最大流是存在的)，那么肯定不存在自 $s$ 到 $t$ 的特殊路. 注意，被构造出的割$(X_0, Y_0)$是一个最小割(即最小容量割)，这是因为对任意割$(X, Y)$，$c(X, Y)\geqslant|f_0|$. 结合上述观察，证明下述著名的 Ford and Fulkerson(1956)定理.

**定理 7.1** *在运输网络中，所有流 $f$ 上 $|f|$ 的最大值，等于所有割$(X, Y)$中 $c(X, Y)$的最小值.*

这个定理通常称为"最大流-最小割"定理. 上述我们使用的增加一个流的强度的方法，在某种程度上给出了更多的信息.

**定理 7.2** *在一个运输网络中，如果所有容量都是整数，那么存在一个最大强度的流 $f$，使所有的 $f(e)$都为整数.*

**证明** 从 0-流开始，论证上述提供的增加流强度的方法，一直达到最大流为止. 在每一步 $\alpha$ 都是整数，因此，下一个流也是整数值. ■

**问题 7A** 对于图 7.1 中的运输网络，构造其一个最大流.

**问题 7B** 运输网络中的一个*初等流*，是这样一个流 $f$，它在从 $s$ 到 $t$ 的一条简单有向路上的每一条边的值均为一个正常数 $\alpha$，而不在该路上的边，其值均为 0. 证明每一个流是若干初等流之和并允许有强度为 0 的流.（这就意味着从 0-流开始，并只用具有前向边的特殊路就能够达到最大流.）构造一个网络及其上的一个非最大流，使其关于这个流不存在仅由前向边组成的自 $s$ 到 $t$ 的特殊路. [64]

**问题 7C** 令$(X_1, Y_1)$和$(X_2, Y_2)$是一个运输网络的两个最小割(即最小容量的割). 证明$(X_1 \cup X_2, Y_1 \cap Y_2)$也是一个最小割.（由第一原理或最大流方法可证明.）

**问题 7D** 由定理 7.1 和定理 7.2，证明霍尔(P. Hall)的婚姻定理，即定理 5.1.

很显然，本章所讨论的专题在实际中是非常重要的. 各类产品的日常计划，依赖于通过运输网络产生最优流的算法. 关于这个领域的算法方面，我们不进行深入讨论. 但对有关伯克霍夫(Birkhoff)定理(即定理 5.5)问题，我们将给出定理 7.2 的一个漂亮的应用. 在给出这个定理及其证明之前，我们注意到，用几个试图归结为定理 5.5 的方法来证明这个定理，但是都没有成功. 下述的证明归功于 A. Schrijver.（在定理 7.3 中，若 $b=v$，则我们有定理 5.5 的情形.）

**定理 7.3** *令 $A$ 是一个 $b\times v$ 阶的(0，1)-矩阵，它的每行有 $k$ 个 1，而每列有 $r$ 个 1(因此 $bk=vr$). 令 $\alpha$ 是一个有理数，$0<\alpha<1$，使得 $k'=\alpha k$，$r'=\alpha r$ 都是整数. 那么存在一个 $b\times v$ 阶的(0，1)-矩阵 $A'$，使 $A'$ 的每行有 $k'$ 个 1，每列有 $r'$ 个 1，并且 $A'$ 的元素 $a'_{ij}=1$ 仅当 $A$ 的对应元素为 1，即 $A'$ 可由 $A$ 中某些 1 变为 0 而得到.*

**证明** 我们构造一个运输网络，其顶点为 $s$(发点)，$x_1$，…，$x_b$(对应于 $A$ 的行)，$y_1$，$y_2$，…，$y_v$(对应于 $A$ 的列)和 $t$(收点). 其边为$(s, x_i)$，它的容量为 $k$，$1\leqslant i\leqslant b$；$(x_i, y_j)$当且仅当 $a_{ij}=1$，这些边的容量均为 1；$(y_j, t)$，它的容量为 $r$，$1\leqslant j\leqslant v$. 这样定义的网络，保证了它有所有边都饱和的最大流. 我们现在把发点的出边的容量改为 $k'$，把收点的入边的容量改为 $r'$. 所有边的容量仍都是整数，并且显然存在一个最大流，它在所有边$(x_i, y_j)$上的值 $f((x_i, y_j))=\alpha$. 根据定理 7.2，也存在最大流 $f^*$，使 $f^*$ 在一切边上的值为整数，即 $f^*((x_i, y_j))=0$ 或 1. 由这个流，我们直接就找出了所要求的矩阵 $A'$. ■ [65]

上述定理可以有几种方式进行推广且其证明思路基本相同，下面是略微不同的推广方式.

对于某些组合应用，使用下述定理是很方便的，这里不需要引进容量或强度概念. 这个定理可由定理 7.2 导出——见 Ford and Fulkerson(1956)，但我们还是给出一个直接证明.

有向图 $D$ 上的一个*循环流*，就是从 $E(D)$到实数集上的一个映射 $f$，使得对每一个顶点 $f$ 满足流的守恒条件. 我们不要求它的非负性，可认为循环流是有向图的关联矩阵的零空间中的向量.

**定理 7.4** *令 $f$ 是有限的有向图 $D$ 的一个循环流，那么存在一个整数循环流 $g$，使得对每一条边 $e$，$g(e)$等于$\lfloor f(e)\rfloor$或者$\lceil f(e)\rceil$.*

我们可以说，$g$ 的值是由 $f$ 的值"舍入"得到的. 当然，若 $f(e)$已经是整数，则 $g(e)=f(e)$.

**证明** 给定循环流 $f$，讨论满足

$$\lfloor f(e)\rfloor \leqslant g(e) \leqslant \lceil f(e)\rceil \tag{7.2}$$

的循环流 $g$，并且在满足式(7.2)的情况下，使 $g(e)$为整数的边尽可能地多.

令 $H$ 是 $D$ 的一个支撑子图，它的边集由非整数的 $g(e)$对应的 $D$ 中的那些边组成，即使得式(7.2)中的两个不等式均为严格不等式的边. 流的守恒条件意味着 $H$ 中没有次为 1 的顶点，因此，如果 $g$ 不是整数，则 $H$ 包含一个多边形.

66 令 $P$ 是 $H$ 的一个多边形，那么过 $P$ 有一条简单的闭路；令 $A$ 是 $P$ 上一些边的集合，这些边是 $D$ 中这条路的前向边；令 $B$ 是 $P$ 中在这条路上的后向边集合. 对任意常数 $c$，我们得到一个新的循环流 $g'$为

$$g'(e):=\begin{cases}g(e)+c & \text{若}\quad e\in A,\\ g(e)-c & \text{若}\quad e\in B,\\ g(e) & \text{若}\quad e\notin E(P).\end{cases}$$

如果 $c$ 很小，那么用 $g'$替换 $g$ 后式(7.2)仍成立. 选取

$$c:=\min\left\{\min_{e\in A}\left(\lceil f(e)\rceil-g(e)\right),\min_{e\in B}\left(g(e)-\lfloor f(e)\rfloor\right)\right\}.$$

那么 $g'$仍满足式(7.2)，并且使 $g'(e)$为整数的边至少增加了一条(在上述表示式中，达到最小值的那一项对应的边). 这就与 $g$ 的选取矛盾. ■

**推论** 令 $f$ 是有限的有向图 $D$ 的一个整数循环流，$d$ 是任意一个正整数，那么 $f$ 可以表示为整数循环流的和 $g_1+g_2+\cdots+g_d$，使得对每一个 $j$ 和每条边 $e$ 有

$$\lfloor f(e)/d\rfloor\leqslant g_j(e)\leqslant\lceil f(e)/d\rceil. \tag{7.3}$$

**证明** 对 $d$ 使用归纳法. 对 $d=1$，结论显然成立.

设 $d\geqslant 2$，将定理 7.4 应用于循环流 $f/d$，对 $j=1$ 求出满足式(7.3)的整数循环流 $g_1$. 应用归纳假设可以得到

$$f-g_1=g_2+g_3+\cdots+g_d,$$

其中对 $j=2, 3, \cdots, d$，$g_j$ 是满足下式的整数循环流：

$$\lfloor(f(e)-g_1(e))/(d-1)\rfloor\leqslant g_j(e)\leqslant\lceil(f(e)-g_1(e))/(d-1)\rceil.$$

一个容易的习题是：如果 $a$ 是一个整数，而 $b$ 是$\lfloor a/d\rfloor$或者$\lceil a/d\rceil$，则

$$\left\lfloor\frac{a}{d}\right\rfloor\leqslant\left\lfloor\frac{a-b}{d-1}\right\rfloor\quad\text{和}\quad\left\lceil\frac{a-b}{d-1}\right\rceil\leqslant\left\lceil\frac{a}{d}\right\rceil,$$

67 由此，上述两个不等式隐含着对 $j=2, 3, \cdots, d$ 式(7.3)成立. ■

由一个 $m\times n$ 阶的实数矩阵 $A$，其中 $A$ 的元素 $a_{ij}$不必非负也不必是整数，我们可以得到一个具有 $m+n+2$ 个顶点和 $mn+m+n+1$ 条边的有向图上的一个循环流. 这个有向图类似于定理 7.3 的证明中使用的那个有向图. 其中顶点 $x_1$，$x_2$，$\cdots$，$x_m$ 对应于 $A$ 的行，而顶点 $y_1$，$y_2$，$\cdots$，$y_n$ 对应于 $A$ 的列，另外两个顶点记为 $s$ 和 $t$. 从 $x_i$ 到 $y_j$ 有一条边，该边上循环流的值为 $a_{ij}$；从 $s$ 到 $x_i$ 的边上循环流的值等于 $A$ 的第 $i$ 行元素的和 $r_i$，从 $y_j$ 到 $t$ 的边上循环流的值等于 $A$ 的第 $j$ 列元素的和 $k_j(i=1, 2, \cdots, m, j=1, 2, \cdots, n)$；另外还有从 $t$ 到 $s$ 的边，

其上循环流的值等于 $A$ 中所有元素的和. 如果用一个标量 $\alpha$ 乘以这个循环流 $f$，对循环流 $\alpha f$ 应用定理 7.4，并且把得到的整数流再翻译为矩阵，那么我们就得到了下述定理的部分(i)，部分(ii)可由推论直接推出.

**定理 7.5** *(i)给定一个矩阵 $A$ 和一个实数 $\alpha$，那么存在一个整数矩阵 $B$，使 $B$ 的元素、$B$ 的行和、$B$ 的列和及 $B$ 的所有元素的和，都是矩阵 $\alpha A$ 的相应值的舍入. (ii)如果 $A$ 是一个整数矩阵，$d$ 是任一个正整数，那么*

$$A = B_1 + B_2 + \cdots + B_d,$$

*其中每一个 $B_i$ 是一个整数矩阵，它的元素、行和、列和及所有元素的和，都是 $\alpha A$ 的相应值的舍入.*

**问题 7E** 证明下述结论都是定理 7.5 的直接结果：(i)问题 5A 的(iii)；(ii)定理 5.5；(iii)定理 7.3；(iv)一个有限图，如果它的每一个顶点的次都是偶数，则它有*均衡定向*，其中每一个顶点的入次和出次都相同；(v)如果一个二部图的最小次为 $\underline{d}$ 且最大次为 $\bar{d}$，那么它的边可以用 $\bar{d}$ 种颜色去染，使其在每一个顶点出现的颜色均不同，而用 $\underline{d}$ 种颜色去染，能够使每一个顶点上出现的颜色均相同.

**问题 7F** 证明一个连通有向图 $D$ 上的所有循环流的向量空间的维数为 $|E(D)| - |V(D)| + 1$.

[68]

## 评注

通常人们不用特殊路这个术语，而是把它称为*增广路*.

如果一个运输网络的所有容量均为整数，那么流的强度每次至少增加一个单位，因此用特殊路方法构造最大流，经过有限次迭代必终止. Ford and Fulkerson(1962)构造了一个具有无理数容量的例子，他们设计出特殊路选取的方式，使其导出流的一个无穷序列，而这些流的强度收敛于最大流的实际强度的四分之一！然而，如果人们每次选取*最短*的特殊路，那么可以证明，最多经过 $O(n^3)$次迭代就能得到最大流，其中 $n$ 为网络的顶点个数. 见 Edmonds and Karp (1972).

求最大流问题是线性规划问题的一个例子，因此可以用线性规划的方法，即单纯形算法求解. 网络流问题的特殊性在于它的矩阵是全幺模的，这也说明了为什么定理 7.2 成立. 关于线性和整数规划的更详细讨论，参见下述有关文献. 图的方法通常比单纯形算法快且更易理解.

在代数拓扑学中，有向图上的循环流被称为 1-圈. 对于任一个全幺模矩阵的零空间中的向量 $f$，类似于定理 7.4 的结论成立.

定理 7.1、定理 7.2、定理 7.4 和算法都有许多组合应用，这是因为某些组合问题可以用运输网络来描述. 例如，求二部图的最大匹配问题，等价于求与其相联系的一个网络的最大(整数)流问题(见参考文献)，因此求最大匹配有一个好算法. 在第 16 章中，我们将进一步应用这些定理解决(0，1)-矩阵的存在性；在第 38 章中将解决集合划分问题.

## 参考文献


69

J. Edmonds and R. M. Karp (1972), Theoretical improvements in algorithm efficiency for network flow problems, *J. Assn. for Computing Machinery* **19**, 248–264.

L. R. Ford, Jr. and D. R. Fulkerson (1962), *Flows in Networks*, Princeton University Press.

T. C. Hu (1969), *Integer Programming and Network Flows*, Addison-Wesley.

70

V. Chvátal (1983), *Linear Programming*, W. H. Freeman.

# 第 8 章　德布鲁因序列

下述问题来源于所谓的*旋转鼓问题*. 先看图 8.1 中的旋转鼓.

鼓上每一段具有两种类型之一，这两种类型分别用 0 和 1 表示. 我们要求鼓的任意相继的 4 段唯一确定这个鼓的位置. 这就意味着，鼓上相继的 0 和 1 组成的 16 种可能的 4 元组，应是 0～15 这 16 个整数的二进制表示. 这个要求能实现吗？如果能，那么有多少种不同的方式？第一个问题是容易回答的. N. G. de Bruijn(1946)讨论了这两个问题，为此，他描述了下面的图以及对应的 0 和 1 的圆序列，通常称这个图为*德布鲁因*(De Bruijn)图，而这个圆序列称为*德布鲁因序列*.

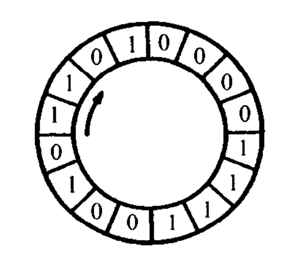


图　8.1

我们构造一个有向图(后面称之为 $G_4$)，它的顶点是所有的 0 和 1 组成的三元组(即 3-比特二进制字)，而顶点 $x_1x_2x_3$ 到顶点 $x_2x_3 0$ 和 $x_2x_3 1$ 有有向边. 弧($x_1x_2x_3$，$x_2x_3x_4$)的标号为 $e_j$，其中 $x_1x_2x_3x_4$ 是整数 $j$ 的二进制表示. 这个图在顶点 000 和 111 各有一个环. 如前述所见，由于这个图每一个顶点的出次和入次都是 2，所以这个图有一条欧拉回路. 这样一条闭路就产生了这个鼓所需要的 16-比特的序列. 这样的(圆)序列就称为德布鲁因序列. 例如，路 000→000→001→011→111→111→110→100→001→010→101→011→110→101→010→100→000 对应于 0000111100101101(首尾相接的圈). 我们称这样的路为完全圈.

71

按上述类似的方法，我们定义 0 和 1 的($n-1$)元组上的有向图 $G_n$(因此 $G_n$ 有 $2^n$ 条边).

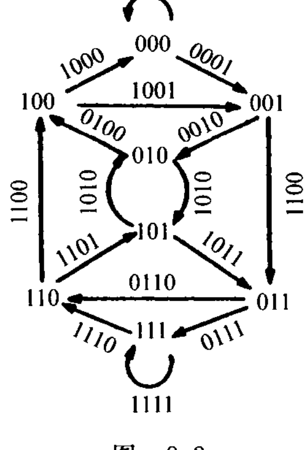



图　8.2

图 8.2 只给出了图 $G_4$. 在这一章里，我们把每一顶点的出次和入次均为 2 的有向图，称为"*2-入 2-出图*"，对于这样一个图 $G$，我们定义 $G$ 的*加倍图* $G^*$ 如下：

(i)对于 $G$ 的每一边对应于 $G^*$ 的一个顶点.

(ii)若 $a$ 和 $b$ 是 $G^*$ 的两个顶点，那么从 $a$ 到 $b$ 有一条边，当且仅当对应于 $a$ 的 $G$ 的边的头与对应于 $b$ 的 $G$ 的边的尾相接.

显然，$G_n^* = G_{n+1}$.

**定理 8.1**　*设 $G$ 是 2-入 2-出图，它有 $m$ 个顶点和 $M$ 个完全圈，则 $G^*$ 有 $2^{m-1}M$ 个完全圈.*

**证明**　对 $m$ 用归纳法证明.

(a)若 $m=1$，则 $G$ 只有一个顶点 $p$，且 $p$ 到 $p$ 有两个环. 那么 $G^* = G_2$，显然它有一个完全圈.

72

(b)假定 $G$ 连通. 如果 $G$ 有 $m$ 个顶点，并且在每一个顶点上都有一个环，那么除掉这些环后，$G$ 是一个回路，如 $p_1 \to p_2 \to \cdots \to p_m \to p_1$. 令 $A_i$ 是 $p_i$ 到 $p_i$ 的环，$B_i$ 是 $p_i \to p_{i+1}$ 的弧. 我们总是用小写字母表示 $G^*$ 中对应的顶点. $G^*$ 的形式如图 8.3 所示.

显然，$G^*$ 中的一个圈从 $b_i$ 到 $b_{i+1}$ 有两种方式. 因此，$G$ 只有一个完全圈时，$G^*$ 有 $2^{m-1}$ 个完全圈.

(c)现在假设 $G$ 有一个顶点 $x$，在 $x$ 上无环. 如图 8.4 表示的情形，其中 $P$，$Q$，$R$，$S$ 是 $G$ 的不同的边(虽然顶点 $a$，$b$，$c$，$d$ 中某一些可能重合).

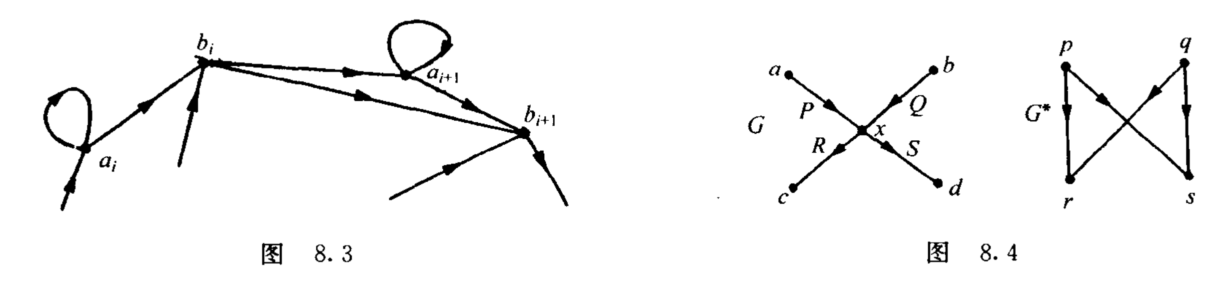



图 8.3　　　　图 8.4

从 $G$ 上去掉顶点 $x$，我们构造一个新的 2-入 2-出图. 这可以按两种方式来做：令 $P=R$ 和 $Q=S$ 得到 $G$；令 $P=S$ 和 $Q=R$ 得到 $G_2$. 然后，按归纳假设，将定理应用到 $G_1$ 和 $G_2$.

$G^*$ 中的完全圈有三种类型，这三种不同的类型依赖于从 $r$ 出发并且分别回到 $p$ 和 $q$ 的两

73

条路是否都到 $p$ 或都到 $q$，或者一条到 $p$ 另一条到 $q$. 我们这里只讨论一种情况，其余两种情况都是类似的，留给读者去完成. 图 8.5 表示的情形是：路 1 是从 $r$ 到 $p$，路 2 是从 $s$ 到 $q$，路 3 是从 $s$ 到 $p$，路 4 是从 $r$ 到 $q$.

由此得到 $G^*$ 中的 4 个完全圈：

$$1,\ pr,\ 4,\ qs,\ 3,\ ps,\ 2,\ qr$$
$$1,\ ps,\ 2,\ qr,\ 4,\ qs,\ 3,\ pr$$
$$1,\ ps,\ 3,\ pr,\ 4,\ qs,\ 2,\ qr$$
$$1,\ ps,\ 2,\ qs,\ 3,\ pr,\ 4,\ qr$$

在 $G_1^*$ 和 $G_2^*$ 里，这种情形简化为图 8.6.

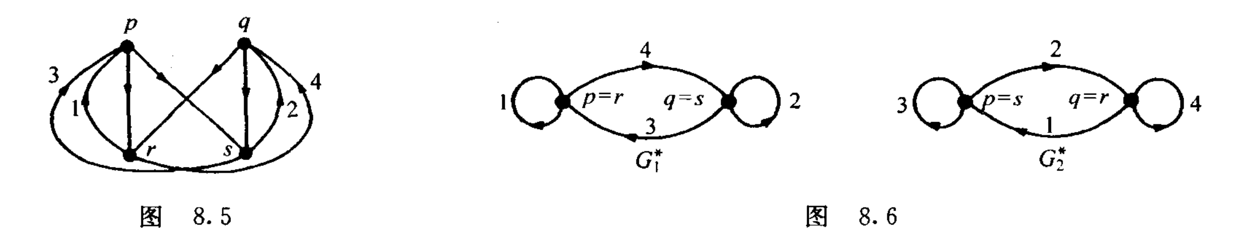



图 8.5　　　　图 8.6

$G_1^*$ 和 $G_2^*$ 中的每一个有一个完全圈，它由 1，2，3 和 4 组成. 对于其余两种情况，我们也能找出 $G_1^*$ 和 $G_2^*$ 中的两个完全圈，它们对应于 $G^*$ 中的 4 个完全圈. 因此，$G^*$ 中完全圈的个数等于 $G_1^*$ 和 $G_2^*$ 中完全圈的个数之和的 2 倍. 另一方面，$G$ 中完全圈的个数显然等于 $G_1$ 和 $G_2$ 中完全圈的个数之和. 因此，由归纳假设定理得证. ■

74

现在我们能够回答一个德布鲁因图有多少个完全圈的问题.

**定理 8.2** $G_n$ 恰有 $2^{2^{n-1}-n}$ 个完全圈.

**证明** 当 $n=1$ 时，定理的结论正确. 由于有 $G_n^*=G_{n+1}$，故按归纳法由定理 8.1 即得本定理的结果. ■

另外一个证明见第 36 章.

**问题 8A** 令 $\alpha$ 是$\mathbb{F}_{2^n}$中的本原元. 对 $1 \leqslant i \leqslant m := 2^n - 1$，令

$$\alpha^i = \sum_{j=0}^{n-1} c_{ij}\alpha^j.$$

证明序列

$$0, c_{10}, c_{20}, \cdots, c_{m0}$$

是德布鲁因序列.

**问题 8B** 找出一个三进制的长为 27 的圆序列(由符号 0，1，2 组成)，使得每一个三进制数字的有序三元组出现在该圆序列的三个相继的位置上. 首先概要地画出 9 个顶点的有向图，使得这个图的欧拉回路对应于这样的序列.

**问题 8C** 我们希望构造一个(指数模 8 的)圆序列 $a_0$，$a_1$，…，$a_7$，使得滑动窗口 $a_i$，$a_{i+1}$，$a_{i+3}$($i=0$，1，…，7)包含每一个可能的有序三元组一次. 证明(而不是用反复试验法)这种希望是不可能的.

**问题 8D** 令 $m := 2^n - 1$. 构造德布鲁因序列 $a_0$，$a_1$，…，$a_m$ 的一个算法如下：开始取 $a_0 = a_1 = \cdots = a_{n-1} = 0$. 对 $k > n$，我们取 $a_k$ 为{0，1}的最大值，并且满足序列($a_{k-n+1}$，…，$a_{k-1}$，$a_k$)在($a_0$，…，$a_{k-1}$)中不作为(相继)子序列出现. 用这个算法得到的序列称为福特(Ford)序列. 证明这个算法的确产生了一个德布鲁因序列.

## 评注

虽然本章中的图通常称为德布鲁因图，但是定理 8.1 是 C. F. Sainte-Marie 在 1894 年证明的，这一结果长时间没有引起人们的注意. 我们引用了 De Bruijn(1975)的工作. [75]

N. G. de Bruijn(1918—)是著名的荷兰数学家之一，他在许多不同领域工作过，如分析、数论、组合学、计算科学和结晶学.

我们特别提一下关于某些荷兰人名的拼音问题. 当去掉 N. G. de Bruijn 开头的大写字母后，就应把 de 写成大写字母，并且在人名表中应列在 B 目之下. 类似地，对 Van der Waerden 名字，当去掉开头的大写字母后，应列在人名表的 W 目之下.

用代数方法证明定理 8.1，请参看第 36 章.

## 参考文献


N. G. de Bruijn (1946), A combinatorial problem, *Proc. Kon. Ned. Akad. v. Wetensch.* **49**, 758–764.

N. G. de Bruijn (1975), Acknowledgement of priority to C. Flye Sainte-Marie on the counting of circular arrangements of $2^n$ zeros and ones that show each $n$-letter word exactly once, T. H. report 75-WSK-06, Eindhoven University of Technology.

C. Flye Sainte-Marie (1894), Solution to question nr. 48, *Intermédiaire des Mathématiciens* **1**, 107–110.


[76]

# 第9章　两个(0，1，*)问题：图的编址和散列编码设计

下述问题来源于通信理论．对一个电话网络而言，终端 $A$ 和 $B$ 之间连通后，消息可沿任一方向传递．对计算机网络而言，希望把消息从 $A$ 传到 $B$，而 $B$ 事先不必知道有消息在传递给它．其想法是让消息按 $B$ 的地址前进，使得在网络的每一个节点对消息的传递方向做出决策．

一个自然的尝试是给图 $G$ 的每一个顶点一个二进制地址，即 $\{0, 1\}^k$ 中的元素，图中两个顶点之间的距离等于这两个顶点的二进制地址的所谓汉明(Hamming)距离，即地址的不相同位的个数．这等价于把 $G$ 视为超立方图 $H_k$ 的诱导子图，这里 $V(H_k):=\{0, 1\}^k$，当两个 $k$ 元有序组只有一个坐标不同时，它们是相邻的，但对 $G=K_3$ 的例子，已证明这样的地址不存在．我们现在引进一个新的字母表 $\{0, 1, *\}$，从这个字母表中取出有序 $n$ 元组来构成地址．两个地址之间的距离定义为一个是 0 另一个是 1 的位的个数(* 对距离无贡献)．确定图 $G$ 的顶点地址就是要求 $G$ 中任何两个顶点之间的距离等于这两个顶点的地址的距离．显然，当 $n$ 足够大时，这是可以做到的．我们用 $N(G)$ 表示在 $G$ 有长度为 $n$ 的地址时 $n$ 的最小值．

77

对于一棵树，我们可以不用符号 * 给出树的地址，其做法如下：使用归纳法．对于两个顶点的树，显然有长度为 1 的地址．假定我们能给出 $k$ 个顶点的树的地址，设 $x_0, x_1, \cdots, x_k$ 是 $k+1$ 个顶点树的顶点，并且 $x_0$ 是 $T$ 的一次顶点，那么从 $T$ 中去掉顶点 $x_0$ 后就得到 $k$ 个顶点的树．按归纳假设，设其顶点 $x_i$ 的地址为 $\boldsymbol{x}_i$，$i=1, 2, \cdots, k$．不妨设 $x_0$ 与 $x_1$ 相邻，那么树 $T$ 的顶点 $x_i$ 的地址为 $(0, \boldsymbol{x}_i)$，$1\leqslant i\leqslant k$，而 $x_0$ 的地址为 $(1, \boldsymbol{x}_1)$．容易验证它们确实是 $T$ 的地址．因此，对一棵树 $T$ 而言，有 $N(T)\leqslant |V(T)|-1$．

第二个例子是讨论 $K_m$．在 $m-1$ 阶单位矩阵中，我们把该矩阵对角线上方的零元素均换为符号 *，然后增加一行，其元素全为零．这样得到的 $m\times(m-1)$ 阶矩阵，其任意两行的距离均为 1，因此，$N(K_m)\leqslant m-1$．

图 9.1

第三个例子是研究图 9.1 中的图．

一个可行(但非最优)的地址是

| 1 | 1 | 1 | 1 | * | * |
|---|---|---|---|---|---|
| 2 | 1 | 0 | * | 1 | * |
| 3 | * | 0 | 0 | 0 | 1 |
| 4 | 0 | 0 | 1 | * | * |
| 5 | 0 | 0 | 0 | 0 | 0 |

我们现在说明图的地址和二次型之间的对应性(这是 Graham and Pollak，1971 的思想)．考虑图 9.1 中的图 $G$ 和上述给出的地址．联系于地址的第一列，我们有一个乘积项$(x_1+x_2)$

$(x_4+x_5)$. 这里当 $i$ 的地址在列 1 中为 1 时，$x_i$ 在第一个因子里，当 $i$ 的地址在列 1 中为 0 时，$x_i$ 在第二个因子里. 如果每一列都有这样一个乘积项，那么把这些乘积项加起来，展开之后就得到一个二次型 $\sum d_{ij}x_ix_j$，其中 $d_{ij}$ 表示顶点 $i$ 和 $j$ 在 $G$ 中的距离. 因此，确定 $G$ 的地址，相当于把二次型 $\sum d_{ij}x_ix_j$ 写为 $n$ 个乘积 [78]

$$(x_{i_1}+\cdots+x_{i_k})(x_{j_1}+\cdots+x_{j_l})$$

之和，使得任一 $x_i$ 不同时出现在这两个因子里. 变量的个数为 $|V(G)|$.

**定理 9.1** 令 $n_+$ 和 $n_-$ 分别表示图 $G$ 的距离矩阵 $(d_{ij})$ 的正特征值和负特征值的个数，则 $N(G)\geqslant\max\{n_+, n_-\}$.

**证明** 上述提到每一个二次型都可以表示为形式 $\frac{1}{2}\boldsymbol{x}^{\mathrm{T}}A\boldsymbol{x}$，其中 $\boldsymbol{x}:=(x_1, x_2, \cdots, x_n)$，而当 $x_ix_j$ 项出现在二次型里时，$A$ 中的元素 $a_{ij}=1$，否则 $a_{ij}=0$. 这样一个矩阵的秩为 2 且其迹为 0. 因此它有一个正特征值和一个负特征值. 由于矩阵 $(d_{ij})$ 是相应的二次型矩阵之和，所以它最多有 $n$ 个正(负)的特征值. ■

**定理 9.2** $N(K_m)=m-1$.

**证明** 我们已证明了 $N(K_m)\leqslant m-1$，由于 $m$ 阶矩阵 $J-I$ 是 $K_m$ 的距离矩阵，并且 $m-1$ 是 $J-I$ 的重数为 1 的特征值，而 $-1$ 为 $J-I$ 的重数为 $m-1$ 的特征值，从而由定理 9.1 可导出本定理的结果. ■

下面我们将证明，一棵树 $T$ 的最短地址的长度为 $|V(T)|-1$.

**定理 9.3** 若 $T$ 是 $n$ 个顶点的树，则 $N(T)=n-1$.

**证明** 首先计算 $T$ 的距离矩阵 $(d_{ij})$ 的行列式. 我们把 $T$ 的顶点编号为 $p_1, \cdots, p_n$，使得 $p_n$ 是端点且相邻于 $p_{n-1}$. 在 $T$ 的距离矩阵中，将其第 $n$ 行减去第 $n-1$ 行. 然后，从第 $n$ 列减去第 $n-1$ 列. 那么这个矩阵的最后一行和最后一列中，除对角线上的元素为 $-2$ 外，其余元素全为 1. 再对顶点 $p_1, \cdots, p_{n-1}$ 重新编号，使新的 $p_{n-1}$ 为 $T\setminus\{p_n\}$ 的端点且相邻于新的 $p_{n-2}$. 然后对 $n-1$ 行和 $n-2$ 行，以及 $n-1$ 列和 $n-2$ 列重复上述过程，经过 $n-1$ 次重复后，我们就得到行列式 [79]

$$\begin{vmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & -2 & 0 & \cdots & 0 \\ 1 & 0 & -2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & -2 \end{vmatrix}.$$

由这个行列式我们得到一个不寻常的结果：$n$ 个顶点树的距离矩阵的行列式 $D_n$ 的表示式为

$$D_n=(-1)^{n-1}(n-1)2^{n-2},$$

即它只依赖于 $|V(T)|$，当我们按上述描述方法对树的顶点进行编号时，其距离矩阵左上方的 $k\times k$ 阶的主子式，是 $k$ 个顶点的子树的距离矩阵. 因此，序列 $1, D_1, D_2, \cdots, D_n$ 等于

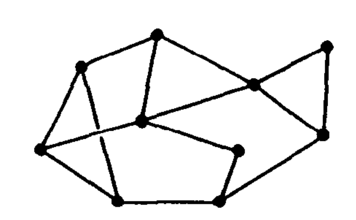
$$1,0,-1,4,-12,\cdots,(-1)^{n-1}(n-1)2^{n-2},$$

其中 $D_k$ 为 $k\times k$ 子式的行列式. 如果我们把符号 0 视为正的，则这个序列里相同符号的两个相继的项只出现一次. 根据二次型的基本定理，可以推出这个相应的二次型有指标 1，因此 $(d_{ij})$

有一个正特征值；参见 B. W. Jones(1950)的定理 4. 这样由定理 9.1 可推出本定理的结果. ■

对所有连通图 $G$，$N(G)\leqslant |V(G)|-1$ 的猜想已由 P. Winkler 于 1983 年证明了. 这个证明是构造性的. 为了说明如何编制地址，我们尚需一些预备知识. 考虑图 9.2 中的图.

80



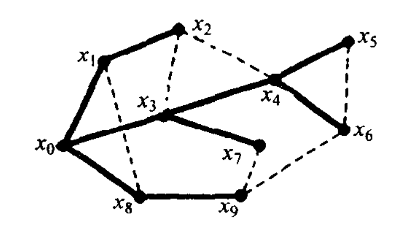



图 9.2

我们选取一个顶点 $x_0$，然后用广度优先搜索法构造一棵支撑树 $T$，再用深度优先搜索法对其顶点编号，所得结果表示在图 9.2 所示的右图中，其中 $E(G)\setminus E(T)$中的边用虚线表示.

令 $n:=|V(G)|-1$. 我们需要几个定义：

对 $i\leqslant n$，定义

$$P(i):=\{j:x_j\text{ 是 }T\text{ 中从 }x_0\text{ 到 }x_i\text{ 路上的顶点}\}.$$

例如，$P(6)=\{0,3,4,6\}$. 令

$$i\triangle j:=\max(P(i)\cap P(j)).$$

对一般情形可表示为图 9.3 中的形式.

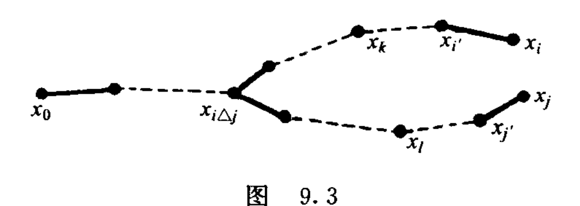



图 9.3

注意，在图 9.3 中，我们有 $i<j$ 当且仅当 $k<l$.

对 $i\leqslant n$，定义

$$i':=\max(P(i)\setminus\{i\}).$$

例如，在图 9.2 中，$7'=3$. 定义

81

$$i\sim j\Leftrightarrow P(i)\subseteq P(j)\text{ 或 }P(j)\subseteq P(i).$$

我们分别用 $d_G$ 和 $d_T$ 表示 $G$ 和 $T$ 中的距离. 定义偏差函数(discrepancy function)$c(i,j)$为

$$c(i,j):=d_T(x_i,x_j)-d_G(x_i,x_j).$$

例如，在图 9.2 中，$c(6,9)=4$.

**引理 9.4**

(i)$c(i,j)=c(j,i)\geqslant 0$.

(ii)若 $i\sim j$，则 $c(i,j)=0$.

(iii)若 $i\not\sim j$，则 $c(i,j')\leqslant c(i,j)\leqslant c(i,j')+2$.

**证明** (i)是显然的；(ii)可由

$$d_G(x_i,x_j) \geqslant |\, d_G(x_j,x_0) - d_G(x_i,x_0) \,| = d_T(x_i,x_j)$$

及 $T$ 的定义导出. (iii)可由下述事实

$$|\, d_G(x_i,x_j) - d_G(x_i,x_{j'}) \,| \leqslant 1,$$
$$d_T(x_i,x_j) = 1 + d_T(x_i,x_{j'})$$

推出. ■

现在我们定义一个图的地址如下：对于 $0 \leqslant i \leqslant n$，定义顶点 $x_i$ 的地址为 $\boldsymbol{a}_i \in \{0, 1, *\}^n$，其中

$$\boldsymbol{a}_i = (a_i(1), a_i(2), \cdots, a_i(n)),$$

而

$$a_i(j) := \begin{cases} 1, & 若\ j \in P(i), \\ *, & 若 \begin{cases} c(i,j) - c(i,j') = 2, \\ c(i,j) - c(i,j') = 1, & i < j, c(i,j)\ 为偶, \\ c(i,j) - c(i,j') = 1, & i > j, c(i,j)\ 为奇, \end{cases} \\ 0, & 其他. \end{cases}$$

**定理 9.5** $d(\boldsymbol{a}_i, \boldsymbol{a}_k) = d_G(x_i, x_k)$.

**证明** 我们可以假定 $i < k$. 分两种情况讨论：$i \sim k$ 和 $i \not\sim k$.

(i)$i \sim k$. 那么 $d_G(x_i, x_k) = |\, P(k) \setminus P(i) \,|$. 对 $j \in P(k) \setminus P(i)$，$j$ 的值恰是 $a_k(j) = 1$，$a_i(j) \neq 1$ 的那些位置. 对 $j$ 的这些值，我们知道 $c(i, j) = 0$，从而，$a_i(j) = 0$. 证毕.

(ii)$i \not\sim k$. 这种情形较难，关键是观察下述事实：令 $n_1 \leqslant n_2 \leqslant \cdots \leqslant n_l$ 是非减的整数序列，使得对每一个 $i$ 有 $|\, n_{i+1} - n_i \,| \leqslant 2$. 若 $m$ 是 $n_1$ 和 $n_l$ 之间的一个偶整数并且不出现在这个序列里，那么存在 $i$，使 $n_i = m - 1$，$n_{i+1} = m + 1$. 现在讨论序列 [82]

$$c(i,k) \geqslant c(i,k') \geqslant c(i,k'') \geqslant \cdots \geqslant c(i, i \triangle k) = 0.$$

按 $a_i(j)$ 的定义及上述的观察，则 $a_i(j) = *$ 和 $a_k(j) = 1$ 出现的次数，与 $c(i, i\triangle k)$ 和 $c(i, k)$ 间的偶整数的个数一样多；类似地，$a_k(j) = *$ 和 $a_i(j) = 1$ 出现的次数与 $c(i, i\triangle k)$ 和 $c(i, k)$ 间的奇整数的个数一样多. 因此

$$\begin{aligned} d(\boldsymbol{a}_i, \boldsymbol{a}_k) &= |\, P(k) \setminus P(i) \,| + |\, P(i) \setminus P(k) \,| - c(i,k) \\ &= d_T(x_i, x_k) - c(i,k) = d_G(x_i, x_k). \end{aligned}$$ ■

这样一来，我们已证明了下述定理.

**定理 9.6** $N(G) \leqslant |\, V(G) \,| - 1$.

**问题 9A** 如果我们应用上述编制地址的方法，那么在图 9.2 的图中，顶点 $x_2$ 和 $x_6$ 的地址是什么？

**问题 9B** 设 $G$ 是 $2n$ 个点的圈(多边形)，求 $N(G)$.

**问题 9C** 设 $G$ 是 $2n+1$ 个点的圈(多边形)，证明 $N(G) = 2n$. 提示：若 $C_k$ 是一个置换矩阵，其元素 $c_{ij} = 1$ 当且仅当 $j - i \equiv 1 \pmod k$ 且 $\zeta^k = 1$，那么$(1, \zeta, \zeta^2, \cdots, \zeta^{k-1})$是 $C_k$ 的一个特征向量.

* * *

现在我们讨论字母表$\{0, 1, *\}$上关于有序$k$-元组的第二个问题. 我们要研究的主题是由Rivest(1974)引进的并且(不幸地)被称为结合区组设计(associative block design); 关于区组设计的内容见第19章. 一个$ABD(k, w)$是$\{0, 1, *\}^k$中$b := 2^w$个元素的集合, 它具有下述性质: 如果把这些元素排成$b\times k$阶矩阵$C$的行, 那么有

83

(i)$C$的每一行有$k-w$个$*$.

(ii)$C$的每一列有$b(k-w)/k$个$*$.

(iii)$C$中任意两个不同的行之间的距离至少为1.

注意, 这个定义意味着$\mathbb{F}_2^k$中的每一个向量, 恰与$C$中一行的距离为0.

这个问题的来源如下: 考虑一个有$k$-比特二进制字的文件. $\{0, 1, *\}^k$中的每一个序列称为一个部分匹配查询(partial match query). 部分匹配检索问题就是从文件中检索那些在查询指定的比特所在位置上与查询相符的字. (所谓)散列编码设计把一个文件分为$b$个不相交的链表$L_1, L_2, \cdots, L_b$. 一项记录$x$将带着指标$h(x)$存入链表里, 其中$h$是将$\{0, 1\}^k$映射到$\{1, 2, \cdots, b\}$的散列函数. 对于一个给定的部分匹配查询, 必定要搜索某些链表. 被搜索的链表个数的最坏情况分析, 引出了$ABD$概念. 在这种情况下, $h(x)$是$C$中到$x$的距离为0的唯一一行的指标.

**例 9.1** 下述矩阵是一个$ABD(4, 3)$:

$$\begin{bmatrix} * & 0 & 0 & 0 \\ 0 & * & 1 & 0 \\ 0 & 0 & * & 1 \\ 0 & 1 & 0 & * \\ * & 1 & 1 & 1 \\ 1 & * & 0 & 1 \\ 1 & 1 & * & 0 \\ 1 & 0 & 1 & * \end{bmatrix}.$$

我们首先证明一个$ABD$的某些基本性质.

**定理 9.7** *如果$ABD(k, w)$存在, 则:*

*(1)它的每一列恰有$bw/(2k)$个0和$bw/(2k)$个1.*

*(2)对$\mathbb{F}_2^k$中的每一个$x$, $C$中与$x$有$u$个位置相同的行恰有$\binom{w}{u}$个.*

*(3)参数满足*

84

$$w^2 \geqslant 2k\left(1-\frac{1}{b}\right).$$

*(4)对任一行, 与该行的$*$号位置相同的行数为偶数.*

**证明** 令$C$是一个$ABD(k, w)$.

(1)$C$中的一行在列$j$具有$*$(或0), 表示到$\mathbb{F}_2^k$中$2^{k-w-1}$(或$2^{k-w}$)个元素的距离均为0. 由定义中的(i)和(ii), 可推出列$j$包含$bw/(2k)$个0.

(2)令 $x\in\mathbb{F}_2^k$，$n_i$ 表示 $C$ 中与 $x$ 恰在 $i$ 个位置上有相同的行的数目．$\mathbb{F}_2^k$中有 $\binom{k}{l}$ 个向量，它们与 $x$ 恰有 $l$ 个位置是相同的．因此，$\binom{k}{l}=\sum n_i\binom{k-w}{l-i}$．即

$$(1+z)^k=(1+z)^{k-w}\cdot\sum n_i z^i.$$

这就证明了 $n_i=\binom{w}{i}$．

(3)由(1)知，$C$ 中所有行对之间的距离之和为 $k\left(\frac{bw}{2k}\right)^2$．由于 $C$ 中任两行之间的距离至少为 1，所以这个和至少为 $\binom{b}{2}$．从而得到结论(3)．

(4)考虑 $C$ 的一行，计算$\mathbb{F}_2^k$中这样一些向量的个数，即这些向量在该行 * 号位置上是 0．具有不同的 * 号模式的每一行代表有偶数个这样的向量，而具有相同 * 号模式的行恰表示一个这样的向量． ■

注意，定理 9.7 中，性质(1)蕴涵着存在 $ABD(k，w)$的必要条件是，$k$ 能整除 $w\cdot 2^{w-1}$．

下述是 A. E. Brouwer(1999)强化了的定理 9.7(3)．

**定理 9.8** *令 $C$ 是一个 $ABD(k，w)$且 $w>3$．*

*(1)如果 $C$ 的两行，除一个位置外，其余都相同，那么*

$$\binom{w}{2}\geqslant k.$$

*(2)否则 $w^2>2k$．*

85

**证明** 设 $c_1$ 和 $c_2$ 是 $C$ 的两行，它们只在位置 1 上是不同的，那么 $C$ 的所有其余的行，必须在某些其余的位置上与 $c_1$ 不同．因此，按定义中的(i)和定理 9.7(3)，我们有

$$b-2\leqslant(w-1)\cdot\frac{bw}{2k}.$$

为了证明结论(1)，我们必须证明这个不等式的右端不可能等于 $b-2$ 或 $b-1$．因为在这两种情况下，等式将意味着$2^{w-1}\mid k$，此时与定理 9.7 矛盾，除非 $w=4$，但这种情形用代换可以排除．

(ii)考虑 $C$ 中 * 模式相同的两行，按假设这两行至少在两个位置上是不同的．那么这两行中的一行到其余各行的距离之和至少为 $2+(b-2)=b$，并且由定理 9.7.1，它等于 $w\cdot(bw)/(2k)$．因此 $w^2\geqslant 2k$，我们必须证明等式不可能成立．按上述论证，等式将意味着具有 * 模式相同的行成对出现，每一对的距离为 2，另外，其余各行到每一对中的两行的距离为 1．不失一般性，设某对中的两行为

$$(*\ *\cdots*00\cdots000)\text{和}(*\ *\cdots*00\cdots011).$$

末位为 1 的还有 $bw/(2k)-1$ 行，这些行末两位必为 01，这是因为，否则它们到上述后面一行的距离为 0 或者到前面一行的距离$>1$．类似地，有 $bw/(2k)-1$ 行，其末两位为 10．因为有距离为 2 的行，所以必有 $bw/(2k)-1=1$．因此，$2^w=2w$，显然当 $w\geqslant 3$ 时，这是不可能的． ■

**推论** *不存在 $ABD(8，4)$．*

应用这些结果，很容易找出 $w \leqslant 4$ 的所有 $ABD(k, w)$. 当然，$w=0$ 是平凡的，对于 $w=1$，2 或 4，则必有 $k=w$(没有 *). 若 $w=3$，那么或者 $k=3$(此时无 *)或者 $k=4$. 在这种情况下 $ABD$ 有两种类型，其中一个就是例 9.1 所示.

**问题 9D** 构造一个 $ABD(4, 3)$，使其前四行与例 9.1 的前四行相同，但其余行不同.

86

在 1987 年，La Poutré 和 Van Lint 证明了 $ABD(10, 5)$是不存在的，而 $ABD(8, 5)$存在的可能性不大，但要证明它是相当困难的. 1999 年 D. E. Knuth 问 Brouwer，除早期的一些结果外，在这个领域里是否有一些新的进展，这件事使 Brouwer 下决心解决这个问题. 在 Brouwer(1999)里可以找到一个例子. 这个例子似乎没有什么规律性结构，现在有一个最小的未决问题是，$ABD(12, 6)$是否存在.

我们现在描述某些构造性方法. 这些构造方法的某些思想将在其他章里用到.

**定理 9.9** *对 $i=1, 2$，若 $ABD(k_i, w_i)$存在，则 $ABD(k_1k_2, w_1w_2)$存在.*

**证明** 我们假设 $w_2>0$. 将 $ABD(k_2, w_2)$的行划分为行数相等的两类 $R_0$ 和 $R_1$. 在 $ABD(k_1, w_1)$中，其每个 * 用具有 $k_2$ 个 * 的行替换，每个 0 用 $R_0$ 的一行替换，每个 1 用 $R_1$ 的一行替换，这种替换是对一切可能的方式进行的. 容易计算，替换后的矩阵是一个 $ABD(k_1k_2, w_1w_2)$. ■

**推论** *$ABD(4^t, 3^t)$存在.*

为了证明下述定理，我们引进一个新的符号，即－. 由符号 0，1，*，－组成的 $k$ 元有序组，表示由 0，1，* 组成的所有这样一些 $k$ 元有序组，即这些 $k$ 元有序组可以用 0 或 1 替换－而得到.

**定理 9.10** *令 $w>0$，假如 $ABD(k, w)$存在，其中 $k=k_0 \cdot 2^t$，$k_0$ 为奇数. 那么对 $0 \leqslant i \leqslant (k-w)/k_0$，$ABD(k, w+ik_0)$存在.*

**证明** 只讨论 $i=1$ 的情况就足够了. 令 $C$ 是一个 $ABD(k, w)$. 定义一个与 $C$ 的阶数相同的矩阵 $A$，使得若 $C_{ij}=*$，则 $a_{ij}=1$，而其余情况 $a_{ij}=0$. 按定理 7.3，$A$ 是两个矩阵 $A_1$ 和 $A_2$ 的和，其中 $A_1$ 每行有 $k_0$ 个 1 且每列有 $2^{w-t}$个 1. 在 $C$ 的一行里的 *，如果在 $A_1$ 里对应这个 * 的位置为 1，那么在 $C$ 里用－替换 *，这样就得到所要求的 $ABD(k, w+k_0)$. ■

**定理 9.11** *如果 $ABD(k, w)$存在，且 $\alpha \geqslant 1$ 使 $\alpha k$ 和 $\alpha w$ 是整数，那么 $ABD(\alpha k, \alpha w)$存在.*

**证明** 只要证明 $ABD(k+l, w+m)$存在就足够了，其中$(k+l)/(w+m)=k/w$ 且$(l, m)=1$.

87

令 $k=k_0 \cdot 2^e$，$k_0$ 为奇数. 由定义中的(ii)知 $k_0 \mid w$. 因此，$wl=mk$ 及$(l, m)=1$ 蕴涵着 $l$ 是 2 的幂. 考虑一个 $l \times l$ 阶的循环矩阵，它的第一行有 $l-m$ 个 * 和 $m$ 个－. 因为 $l$ 整除 $b$，我们可以在 $ABD(k, w)$的矩阵 $C$ 上附加 $b/l$ 个这个循环矩阵的拷贝组成的一列. 容易验证，这个大矩阵就是一个 $ABD(k+l, w+m)$. ■

**例 9.2** 由定理 9.9 的推论，我们有 $ABD(64, 27)$. 定理 9.10 说明对 $27 \leqslant w \leqslant 64$，$ABD(64, w)$存在. 特别地，存在 $ABD(64, 32)$. 这样，定理 9.11 蕴涵着对一切 $w \geqslant 32$，$ABD(2w, w)$存在. 前面已提到，对 $w=4$ 和 $w=5$ 不存在这样的 $ABD$，而对 $w=6$ 的情况仍没有解决.

## 评注

本章讨论的第一个问题，是贝尔实验室的 J. R. Pierce 提出来的，称之为闭路开关问题. 一些人(包括本书的作者之一)力图去解决它，但没有成功. R. L. Graham 提出给予 200 美元征解后不久，P. Winkler 就解决了这个问题. Winkler 说，在他的证明中的顶点标号的思想，是由于他的计算机科学背景的通常习惯，这是值得注意的. 从整个证明来看，标号的确起了关键作用.

## 参考文献

A. E. Brouwer (1999), An Associative Block Design $ABD(8,5)$, *SIAM J. Comput.* **28**, 1970–1971.

R. L. Graham and H. O. Pollak (1971), On the addressing problem for loop switching, *Bell System Tech. J.* **50**, 2495–2519.

B. W. Jones (1950), *The Theory of Quadratic Forms*, Carus Math. Monogr. **10**, Math. Assoc. of America.

J. A. La Poutré and J. H. van Lint (1985), An associative block design $ABD(10,5)$ does not exist, *Utilitas Math.* **31**, 219–225.

P. Winkler (1983), Proof of the squashed cube conjecture, *Combinatorica* **3**, 135–139.

88

# 第 10 章　容斥原理和反演公式

前几章我们已见到，许多组合分析中的问题都涉及某些对象的计数，我们现在讨论计数中最有用的方法之一，称之为容斥原理．其思想如下：如果 $A$ 和 $B$ 是 $S$ 的子集，我们希望计算出 $S\setminus\{A\cup B\}$中的元素个数，然而其元素个数并不等于 $|S|-|A|-|B|$，这是因为 $A\cap B$ 中的元素被减去了两次．所以其正确答案为 $|S|-|A|-|B|+|A\cap B|$．下述定理是这一思想的推广．

**定理 10.1**　令 $S$ 是一个 $N$-集；$E_1$，…，$E_r$ 是 $S$ 的子集，但不必不同．对集合$\{1,\cdots,r\}$的任一个子集 $M$，我们记 $S$ 在 $\bigcap_{i\in M}E_i$ 中的元素个数为 $N(M)$，并且对 $0\leqslant j\leqslant r$，定义 $N_j:=\sum_{|M|=j}N(M)$．那么 $S$ 中不在诸子集 $E_i(1\leqslant i\leqslant r)$里的元素个数为

$$N-N_1+N_2-N_3+\cdots+(-1)^rN_r. \tag{10.1}$$

**证明**　(i)若 $x\in S$ 且 $x$ 不在任何 $E_i$ 中，那么 $x$ 对表示式(10.1)的贡献为 1.

(ii)如果 $x\in S$ 且 $x$ 恰在 $k$ 个 $E_i$ 里，那么 $x$ 对表示式(10.1)的贡献为

$$1-\binom{k}{1}+\binom{k}{2}-\cdots+(-1)^k\binom{k}{k}=(1-1)^k=0. \qquad ■$$



**注记**　如果在(10.1)的和式中，截去一个正项(负项)的后面部分，那么得到 $S$ 中不在任意 $E_i$ 里的元素个数的上(下)界．

由于这一方法是非常重要的，所以我们举一些例子加以说明．

**例 10.1**　令 $d_n$ 表示 1，2，…，$n$ 的一些排列 $\pi$ 的数目，使得对一切 $i$，$\pi(i)\neq i$(这些排列称为更列排列)．令 $S:=S_n$，且令 $E_i$ 是使 $\pi(i)=i$ 的一些排列 $\pi$ 的子集，按(10.1)，我们有

$$d_n=\sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)!=n!\sum_{i=0}^{n}\frac{(-1)^i}{i!}. \tag{10.2}$$

由这个公式可见，当 $n$ 很大时，一个排列是更列排列的概率接近于 $e^{-1}$．对于 $n$ 和 $n-1$，由公式(10.2)可导出 $d_n$ 的递推公式：

$$d_n=nd_{n-1}+(-1)^n. \tag{10.3}$$

公式(10.2)还可以通过如下的反演得到．考察幂级数 $D(x):=\sum_{n=0}^{\infty}d_n\frac{x^n}{n!}(d_0=1)$．如果我们令 $F(x):=e^xD(x)$，那么

$$F(x)=\sum_{m=0}^{\infty}\left(\sum_{r=0}^{m}\binom{m}{r}d_{m-r}\right)\frac{x^m}{m!}.$$

又因为 $\sum_{r=0}^{m}\binom{m}{r}d_{m-r}=m!$，所以有 $F(x)=(1-x)^{-1}$，从而有 $D(x)=e^{-x}(1-x)^{-1}$，并且对这两个因子展成幂级数后相乘又可导出公式(10.2)．

**例 10.2**　令 $X$ 是 $n$-集，$Y=\{y_1,\cdots,y_k\}$是 $k$-集，我们计算 $X$ 到 $Y$ 的满射的数目．令 $S$

是 $X$ 到 $Y$ 的所有映射的集合，$E_i$ 是使 $y_i$ 不在 $X$ 的象里的那些映射的集合. 根据(10.1)，满射的数目为

$$\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n.$$

显然，若 $k>n$，这个数为 0；若 $k=n$，这个数为 $n!$. 因此，我们就证明了

$$\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n=\begin{cases}n! & 若\ k=n,\\ 0 & 若\ k>n.\end{cases} \tag{10.4}$$

90

像(10.4)这样类型的公式有很多，要直接证明它们都是很困难的. $(-1)^i$ 的出现通常象征着，应用容斥原理于适当对象能产生公式. 例如，本例就是这样. 毫无疑问，在这种情况下观察另外一个证明是很有意义的.

令 $P(x)$ 是一个 $n$ 次多项式，其最高次项的系数为 $a_n$，我们用 $\boldsymbol{P}$ 表示值为 $P(0)$，$P(1)$，…的序列. 现在考虑差序列 $P(1)-P(0)$，$P(2)-P(1)$，…，用 $\boldsymbol{Q}_1$ 表示这个序列，其中 $Q_1(x):=P(x+1)-P(x)$ 是 $n-1$ 次多项式，其最高次项的系数为 $na_n$. 经过多次重复这个过程后，我们得到一个序列 $\boldsymbol{Q}_k$，它的项是

$$\sum_{i=0}^{k}(-1)^i\binom{k}{i}P(x+k-i),$$

对应于 $n-k$ 次多项式 $Q_k(x)$，其最高次项的系数为 $n(n-1)\cdots(n-k+1)a_n$. 如果 $k=n$，则 $\boldsymbol{Q}_k$ 的所有项都是 $n!\ a_n$，若 $k>n$，则它们都是 0. 取 $P(x)=x^n$，我们再次得到公式(10.4).

**例 10.3** 下述恒等式是众所周知的二项式系数之间的关系.

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}\binom{m+n-i}{k-i}=\begin{cases}\dbinom{m}{k} & 若\ m\geqslant k,\\ 0 & 若\ m<k.\end{cases} \tag{10.5}$$

我们知道，如果应用容斥原理来证明这个公式，那么要排除这样的一些集合 $E_i$，即它们含有 $n$-集中的 $i$ 个元素及某个 $m+n-i$ 个元的集合中的 $k-i$ 个元素. 这就说明下述组合问题将导出结果(10.5). 考虑集合 $Z=X\cup Y$，其中 $X=\{x_1, x_2, \cdots, x_n\}$ 是蓝色点的 $n$-集，$Y$ 是红色点的 $m$-集. 那么仅由红色点组成的 $k$-子集有多少个？显然(10.5)的右端就是问题的答案. 如果令 $S$ 是 $Z$ 的所有 $k$-子集的集合，令 $E_i$ 是含有 $x_i$ 的 $k$-子集的集合，那么(10.1)式就是(10.5)的左端.

我们还可以问，是否能够直接证明这个结果？答案是肯定的. 为此，我们利用下述展式：

$$\sum_{j=0}^{\infty}\binom{a+j}{j}x^j=(1-x)^{-a-1}. \tag{10.6}$$

91

注意，在 $(1-x)^n$ 的展式中，$x^i$ 的系数为 $(-1)^i\binom{n}{i}$. 由(10.6)我们发现，在 $(1-x)^{k-m-n-1}$ 的展式中，$x^{k-i}$ 的系数是 $\binom{m+n-i}{k-i}$. 因此，(10.5)的左端是 $(1-x)^{k-m-1}$ 的展式中 $x^k$ 的系数.

如果 $m\leqslant k-1$，显然它是 0，而当 $m\geqslant k$ 时，再由(10.6)知它是 $\binom{m}{k}$.

**例 10.4**(欧拉函数) 令 $n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ 是正整数，用 $\phi(n)$表示小于等于 $n$ 且与 $n$ 互素的正整数的个数，即使得 g. c. d. $(n,\ k)=1$ 且 $1\leqslant k\leqslant n$ 的整数 $k$ 的个数. 取 $S:=\{1,\ 2,\ \cdots,\ n\}$，$E_i$ 是能被 $p_i$ 整除的 $S$ 中元素的集合，其中 $1\leqslant i\leqslant r$，应用定理 10.1. 那么此时(10.1)变为

$$\phi(n)=n-\sum_{i=1}^{r}\frac{n}{p_i}+\sum_{1\leqslant i<j\leqslant r}\frac{n}{p_ip_j}-\cdots=n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right). \tag{10.7}$$

下述定理是经常被引用的.

**定理 10.2** $\sum_{d|n}\phi(d)=n.$

**证明** 设$\{1,2,\cdots,n\}=N$,对每一个 $m\in N$,我们有$(m,n)\mid n$. 使$(m,n)=d$,即 $m=m_1d$, $n=n_1d$ 且$(m_1,n_1)=1$ 的整数 $m$ 的个数显然等于$\phi(n_1)=\phi(n/d)$. 因此 $n=\sum_{d|n}\phi(n/d)$，这等价于定理的结论. ■

在此我们引进所谓的默比乌斯函数，这个函数是很有用的：

$$\mu(d):=\begin{cases}1 & \text{若 } d \text{ 是偶数个不同素数之积},\\ -1 & \text{若 } d \text{ 是奇数个不同素数之积},\\ 0 & \text{其余,即 } d \text{ 不是无平方因子的}.\end{cases} \tag{10.8}$$

**定理 10.3**

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{若 } n=1,\\ 0 & \text{其余}.\end{cases}$$

[92]

**证明** 若 $n=1$，结论显然成立. 若 $n=p_1^{a_1}\cdots p_r^{a_r}$，则由(10.8)我们有

$$\sum_{d|n}\mu(d)=\sum_{i=0}^{r}\binom{r}{i}(-1)^i=(1-1)^r=0.$$ ■

注意，定理 10.1 和定理 10.3 的证明是多么类似！

应用默比乌斯函数，可以将(10.7)改写为

$$\frac{\phi(n)}{n}=\sum_{d|n}\frac{\mu(d)}{d}. \tag{10.9}$$

**问题 10A** 小于 1000 的正整数中，有多少个正整数不含有 1 和 10 之间的数为其因子？

**问题 10B** 在$\mathbb{F}_p[x]$中有多少个首项系数为 1 的 $n$ 次多项式，使得对 $x\in\mathbb{F}_p$ 它们的取值不为 0?

**问题 10C** 求$\sum_{n\leqslant x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor$.

**问题 10D** 在复分析中，最有名的函数之一是所谓的黎曼 ζ-函数，即 $\zeta(s):=\sum_{n=1}^{\infty}n^{-s}$，它定义在 $\mathrm{Re}(s)>1$ 的复平面上. 证明 $1/\zeta(s)=\sum_{n=1}^{\infty}\mu(n)n^{-s}$.

**问题 10E** 设 $f_n(z)$ 是这样一个函数，它把使得 $\eta^n=1$ 但对一切 $1\leqslant k<n$，$\eta^k\neq 1$ 的所有数 $\eta$ 作为它的零点，证明

$$f_n(z)=\prod_{k\mid n}(z^k-1)^{\mu(n/k)}.$$

定理 10.3 能导出一个十分有用的反演公式，称为默比乌斯反演公式.

**定理 10.4** 设 $f(n)$ 和 $g(n)$ 是定义在所有正整数 $n$ 上的函数且满足

$$f(n)=\sum_{d\mid n}g(d). \tag{10.10}$$

93

那么 $g$ 满足

$$g(n)=\sum_{d\mid n}\mu(d)f\left(\frac{n}{d}\right). \tag{10.11}$$

**证明** 由(10.10)，我们有

$$\begin{aligned}\sum_{d\mid n}\mu(d)f\left(\frac{n}{d}\right)&=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)f(d)\\&=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)\sum_{d'\mid d}g(d')=\sum_{d'\mid n}g(d')\sum_{m\mid(n/d')}\mu(m).\end{aligned}$$

由定理 10.3 知，除非 $d'=n$，上式右端的内和是 0，此时就是式(10.11). ■

**注记** 等式(10.11)也蕴涵等式(10.10).

**例 10.5** 我们将计算 0，1 圆序列的数目 $N_n$，其中由旋转得到的两个圆序列被认为是相同的. 令 $M(d)$ 是长为 $d$ 且非周期的圆序列的个数，那么 $N_n=\sum_{d\mid n}M(d)$. 我们观察到所有可能的圆序列数为 $\sum_{d\mid n}dM(d)=2^n$. 由定理 10.4，由这个等式得到

$$nM(n)=\sum_{d\mid n}\mu(d)2^{n/d},$$

因此有

$$\begin{aligned}N_n&=\sum_{d\mid n}M(d)=\sum_{d\mid n}\frac{1}{d}\sum_{l\mid d}\mu\left(\frac{d}{l}\right)2^l\\&=\sum_{l\mid n}\frac{2^l}{l}\sum_{k\mid\frac{n}{l}}\frac{\mu(k)}{k}=\frac{1}{n}\sum_{l\mid n}\phi\left(\frac{n}{l}\right)2^l.\end{aligned} \tag{10.12}$$

最后这个表示式的优点是，它的所有项都是正的. 这就提出一个问题，我们能否采用其他的计数方法得到这个表示式. 我们将看到，下述定理(称为伯恩赛德引理，实际上该定理应归功于柯西(Cauchy)和弗罗贝尼乌斯(Frobenius)，见评注)给出了这个答案.

94

**定理 10.5** 令 $G$ 是作用在集合 $X$ 上的置换群. 对 $g\in G$，令 $\psi(g)$ 表示在 $g$ 下 $X$ 中的不动点的数目，那么 $G$ 的轨道数等于 $\frac{1}{|G|}\sum_{g\in G}\psi(g)$.

**证明** 计算元素对 $(g,x)$ 的数目，其中 $g\in G$，$x\in X$，$x^g=x$. 由置换 $g$ 出发，我们可算出这样的元素对有 $\sum_{g\in G}\psi(g)$ 个. 另一方面，由每一 $x\in X$，这样的元素对有 $|G|/|O_x|$ 个，其中 $O_x$ 为 $x$ 的轨道. 因此，这样的元素对总数为 $|G|\sum_{x\in X}1/|O_x|$. $G$ 的所有轨道构成 $X$ 的一个划

分，并且若对一个轨道中的所有 $x$ 求 $1/|O_x|$ 的和，则这个和为 1. 因此 $\sum_{x\in X} 1/|O_x|$ 为 $G$ 的轨道数. ■

**例 10.5**(续) 设 $G$ 是 $n$ 阶循环群，即一个 0 和 1 的圆序列的旋转群. 如果 $d \mid n$，则存在 $\phi(n \mid d)$ 个整数 $g$，使得 $(n, g)=d$ 且对每一个这样的 $g$，存在 $2^d$ 个圆序列，使旋转 $g$ 个位置它们不动. 因此，定理 10.5 直接推出结果(10.12).

**例 10.6** 下述是 Lucas 在 1891 年提出的著名的“夫妻问题”. 我们希望 $n$ 对夫妻围圆桌就坐，使得男女座位交错且每对夫妻不相邻，那么有多少种不同的就坐方案？我们假定这些女人已在交错座位上坐好，把女人们编号为 1 到 $n$，相应地她们的丈夫也编号为 1 到 $n$. 上述问题相当于把这 1 到 $n$ 的整数放到具有标号 1 到 $n$ 的圆周的位置上，使得对每一个整数 $i$ 不在位置 $i$ 或 $i+1$(模 $n$). 令 $E_i$ 表示丈夫 $i$ 坐在他妻子旁边的就坐方式的集合. 我们要利用容斥原理，因此必须计算有 $r$ 个丈夫坐在各自妻子的旁边有多少种可能的就坐方式. 设有 $A_r$ 种就坐方式，$A_r$ 的计算如下：考虑 $2n$ 个位置的圆序列. 如果丈夫 $i$ 坐在他妻子的右侧，那么这个圆序列的位置 $2i-1$ 上放一个 1；如果丈夫 $i$ 坐在他妻子的左侧，则在位置 $2i$ 上放一个 1；其他情况均放 0. 我们要计算的构形的数目，就是具有 $r$ 个 1 且任何两个 1 不相邻的 $2n$ 个 0 和 1 的圆序列的个数. 令 $A'_r$ 表示从 1 开始(接着为 0)的序列的数目，把 10 作为一个符号，易见我们必须从 $2n-r-1$ 个位置上选取 $r-1$ 个位置. 为计算以 0 开始的序列个数 $A''_r$，我们把 0 放在末尾，这就相当于从 $2n-r$ 个位置上选取 $r$ 个位置，因此

95

$$A_r = A'_r + A''_r = \binom{2n-r-1}{r-1} + \binom{2n-r}{r} = \frac{2n}{2n-r}\binom{2n-r}{r}.$$

由(10.1)，我们知道安排男人座位的方式数为

$$\sum_{r=0}^{n}(-1)^r(n-r)!\binom{2n-r}{r}\frac{2n}{2n-r}. \qquad (10.13)$$

**问题 10F** 我们把整数 1 到 $2n$ 染红色或蓝色，使得若 $i$ 染红色，则 $i-1$ 不能是蓝色. 证明染色的方式数为

$$\sum_{k=0}^{n}(-1)^k\binom{2n-k}{k}2^{2n-2k} = 2n+1.$$

你能直接证明这个恒等式吗？

**问题 10G** 计算整数 1 到 $2n$ 的这样一些排列 $x_1$，$x_2$，…，$x_{2n}$ 的数目，使得对每一个 $i$，$x_i+x_{i+1}\neq 2n+1$，$i=1$，2，…，$2n-1$.

**问题 10H** 对 $0\leqslant k\leqslant n$，证明

$$\sum_{i=0}^{k}\binom{k}{i}D_{n-i} = \sum_{j=0}^{n-k}(-1)^j\binom{n-k}{j}(n-j)!.$$

## 评注

容斥原理早在 1854 年 Da Silva 的文章中出现，后来在 1883 年 Sylvester 的文章也出现过. 因此公式(10.1)及类似的公式有时称为 Da Silva 公式或 Sylvester 公式，而一个常用的且更好

的名字是"筛法公式". 这个公式的确是在数论中广泛应用的典型例子，且称为"筛法". 大部分读者大概都熟悉的一个例子是 Eratosthenes 的筛法：要找出小于等于 $n^2$ 的素数，取小于等于 $n^2$ 的整数且筛出所有小于等于 $n$ 的素数的倍数.

96

在例 10.1 中讨论的更列排列，在后面的例 14.1 和例 14.10 中还要出现. 这个问题首次出现在关于机会博奕早期的一本书《Essai d'analyse sur les jeux de hazard》中，作者为 P. R. de Montmort(1678—1719). 现在还常常使用作者给出的名字"problème des rencontres". 公式(10.2)有时叙述为：如果 $n$ 个人每人存放一把雨伞(一个典型的荷兰人的例子，因为在荷兰经常有雨)，且此后在黑暗(无灯光)中每人随机地取走一把雨伞，那么每一个人都没有拿到自己存放的雨伞的概率粗略地为 $e^{-1}$(若 $n$ 充分大).

例 10.2 中的第二个证明是数值分析中广泛使用的差分法的一个例子.

默比乌斯(A. F. Möbius)(1790—1868)是一位天文学家(此前是高斯(Gauss)的一名助手)，他在几何和拓扑学方面做出了重要贡献(如默比乌斯带).

黎曼(G. F. B. Riemann)(1826—1866)是德国哥廷根(Göttingen)大学教授，他在高斯指导下得到了博士学位. 他的许多思想是很出名的，比如黎曼积分、黎曼曲面和黎曼流形，当然还有称为 $\zeta$-函数的零点定位的黎曼假设. 如果他不是如此年轻就去世，我们不知道他还会给我们留下些什么.

在许多书中，定理 10.5 被称为伯恩赛德(Burnside)引理，这是历史的误解，它应归功于诺伊曼(Neumann, 1979). 实际上有许多定理都错误地归功到其他人，这里只是其中的一个例子而已.

卢卡(F. E. A. Lucas)(1842—1891)是法国的一名数论专家，他因数论和趣味数学方面的著作而著名. 他的数论方面的书就包含了例 10.6 的问题. 斐波那契(Fibonacci)数这个名字是卢卡给出的，见第 14 章的评注.

## 参考文献


F. E. A. Lucas (1891), *Théorie des nombres*, Gauthier-Villars, Paris.

P. M. Neumann (1979), A lemma that is not Burnside's, *Math. Scientist*, **4**, 133–141.


97

# 第11章 积 和 式

在介绍本章的主要专题之前，我们先给出定理10.1的一个推广．与定理10.1中一样，令$S$是一个$n$-集，$E_1$，…，$E_r$(不必不同)是$S$的子集．令$\mathbb{F}$是一个域．对每一个元素$a\in S$，我们在$\mathbb{F}$中指定$a$的一个权$w(a)$．对$\{1, 2, \cdots, r\}$的任一个子集$M$，我们定义$M$的权$W(M)$为$S$中在$\bigcap_{i\in M} E_i$里的元素的权之和．对于$0\leqslant j\leqslant r$，我们定义$W_j := \sum_{|M|=j} W(M)$(因此$W_0=\sum_{a\in S} w(a)$)．

**定理11.1** *若$E(m)$表示$S$中恰好包含在$m$个子集$E_i(1\leqslant i\leqslant r)$里的元素的权之和，则*

$$E(m)=\sum_{i=0}^{r-m}(-1)^i\binom{m+i}{i}W_{m+i}. \tag{11.1}$$

**证明** 这个证明与定理10.1的证明几乎相同．如果$x\in S$且$x$恰好包含在$m$个子集$E_i$里，那么$x$对(11.1)中的和的贡献为$w(x)$．如果$x\in S$且$x$恰好属于$m+k$个子集$E_i$，那么$x$对这个和的贡献为

98

$$w(x)\sum_{i=0}^{k}(-1)^i\binom{m+i}{i}\binom{m+k}{m+i}=w(x)\binom{m+k}{k}\sum_{i=0}^{k}(-1)^i\binom{k}{i}=0. \qquad \blacksquare$$

我们现在给出积和式的定义．令$A=(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n)$是一个$n\times n$的矩阵，它的列为$\boldsymbol{a}_j=(a_{1j}, \cdots, a_{nj})^\top$．那么$A$的积和式per $A$定义为

$$\operatorname{per} A := \sum_{\pi\in S_n} a_{1\pi(1)}\cdots a_{n\pi(n)}. \tag{11.2}$$

因此，积和式的定义与行列式的定义一样，只是积不依赖于置换$\pi$的奇偶性．

由这个定义，积和式显然有下述性质：

$$\operatorname{per} A=\operatorname{per} A^\top; \tag{11.3}$$

如果$P$和$Q$是置换矩阵，那么 $\operatorname{per} A=\operatorname{per} PAQ$; (11.4)

$$\operatorname{per} A \text{ 是 } \boldsymbol{a}_j \text{ 的线性函数}, \quad 1\leqslant j\leqslant n. \tag{11.5}$$

当然，per $A$也是$A$的每一行的线性函数．$A$的积和式比$A$的行列式计算起来更加困难．但是由式(11.2)显然可见，按行或列展开是可能的．为此，我们令$A_{ij}$表示由矩阵$A$去掉第$i$行和第$j$列得到的矩阵，则

$$\operatorname{per} A=\begin{cases}\sum_{i=1}^{n} a_{ij}\operatorname{per} A_{ij}, & 1\leqslant j\leqslant n,\\ \sum_{j=1}^{n} a_{ij}\operatorname{per} A_{ij}, & 1\leqslant i\leqslant n.\end{cases} \tag{11.6}$$

下述计算积和式(归功于Ryser)的方法是定理11.1的一个应用．

**定理 11.2** 令 $A$ 是 $n\times n$ 的矩阵，若 $A_r$ 是由 $A$ 去掉 $r$ 个列得到的矩阵，则 $S(A_r)$ 表示 $A_r$ 的行和之积. 我们定义 $\sum_r$ 为对一切可能的 $A_r$，$S(A_r)$ 之值的和. 那么

$$\text{per } A = \sum_{r=0}^{n-1}(-1)^r \sum_r. \tag{11.7}$$

99

**证明** 设 $S$ 是所有乘积 $p=a_{1i_1}\cdots a_{ni_n}$ 的集合. 定义 $w(p):=p$. 定义 $E_j$ 为乘积 $p$ 的集合且 $j\notin\{i_1, \cdots, i_n\}$，那么 $A$ 的积和式等于 $S$ 中不在任何子集 $E_j$ 里的元素的权之和. 因此，(11.7)是(11.1)的一个直接结果. ■

**问题 11A** 应用定理 11.2 证明(10.4).

**注记** 如果 $A_1, \cdots, A_n$ 是集合$\{1, 2, \cdots, n\}$的子集，并且若 $j\in A_i$，则 $a_{ij}=1$，否则$a_{ij}=0$，那么积和式 per $A$ 就是集合 $A_1, A_2, \cdots, A_n$ 的不同代表系的数目.

**例 11.1** 我们发现 $1, 2, \cdots, n$ 的更列排列数的另一个公式. $n$ 阶矩阵 $J-I$ 的积和式显然为 $d_n$，由式(11.7)我们有

$$d_n = \sum_{r=0}^{n-1}(-1)^r\binom{n}{r}(n-r)^r(n-r-1)^{n-r}. \tag{11.8}$$

把项$(n-1-r)^{n-r}$展开且改变和的顺序后，应用公式(10.4)，我们就得到(10.2)的一个复杂的证明.

在 20 世纪 70 年代，关于(0，1)-矩阵的积和式的一些著名的猜想已经得到了证明，且常常是用巧妙的论证. 事实上，这些猜想推动了关于积和式的大部分研究工作. 因此，在这一章和下一章，我们将集中讨论关于这方面的一些结果，作为入门，我们讨论每行每列有两个 1 的(0，1)-矩阵.

**定理 11.3** 若 $A$ 是一个(0，1)-矩阵，且每行每列的和为 2，那么

$$\text{per } A \leqslant 2^{\lfloor \frac{1}{2}n \rfloor}.$$

**证明** 设 $G$ 是一个图，它的顶点对应于 $A$ 的行，它的边对应于 $A$ 的列，且当 $A(i, j)=1$ 时，顶点 $i$ 和边 $j$ 相关联. 这个图 $G$ 是 2 次正则图，并因此它是若干个不相交的多边形的并. 对应于一个多边形的顶点和边的子矩阵(如果需要可进行行或列重排)是一个循环矩阵：

100

$$\begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

(它可能退化为由 1 组成的 2×2 的矩阵). 矩阵 $A$ 就是这样一些矩阵的直和，即这些矩阵中的每一个的积和式为 2. 因为因子数最多为$\left\lfloor \frac{1}{2}n \right\rfloor$个，所以当 $A$ 是$\left\lfloor \frac{1}{2}n \right\rfloor$个阶为 2 的矩阵 $J$ 的直和时，定理中的等式成立. ■

这个基本定理涉及一个矩阵的行和与这个矩阵的积和式之间的关系，并且对下述一些定理同样也是对的. 这就给我们提出了一个困难的问题. 在 1967 年 H. Minc 猜想，如果 $A$ 是一个 (0，1)-矩阵，且行和为 $r_1$，…，$r_n$，那么

$$\text{per } A \leqslant \prod_{j=1}^{n}(r_j!)^{1/r_j}. \tag{11.9}$$

定理 11.2 表明式(11.9)中的等式可能成立. 事实上，如果 $A$ 是一些矩阵 $J_m$ 的直和，那么(11.9)就取等式. 比(11.9)更弱的一些结果已经得到了证明，但这些论证常常很复杂也很长. 这个猜想最终由 L. M. Brégman 于 1973 年证明了. 更惊奇的是，A. Schrijver 后来居上，他在 1977 年对 Minc 的猜想给出了一个漂亮而很短的证明，这个证明依赖于下述引理.

**引理 11.4** 如果 $t_1$，$t_2$，…，$t_r$ 是非负实数，则

$$\left(\frac{t_1+\cdots+t_r}{r}\right)^{t_1+\cdots+t_r} \leqslant t_1^{t_1}\cdots t_r^{t_r}.$$

**证明** 因为 $x\log x$ 是一个凸函数，因此有

[101]

$$\frac{t_1+\cdots+t_r}{r}\log\left(\frac{t_1+\cdots+t_r}{r}\right) \leqslant \frac{t_1\log t_1+\cdots+t_r\log t_r}{r},$$

这就证明了引理. ■

下面我们用(11.6)的下述形式：

$$\text{per } A = \sum_{k,a_{ik}=1} \text{per } A_{ik}.$$

**定理 11.5** 令 $A$ 是一个 $n\times n$ 的(0，1)-矩阵，它的第 $i$ 行有 $r_i$ 个 1，其中 $1\leqslant i\leqslant n$，那么

$$\text{per } A \leqslant \prod_{i=1}^{n}(r_i)!^{1/r_i}.$$

**证明** 对 $n$ 进行归纳证明. 对 $n=1$，定理是平凡的. 假定对 $n-1$ 阶的矩阵定理成立. 其证明思想是估计$(\text{per } A)^{n \text{ per } A}$的值，并且把这个表示式分为若干项的积. 注意到 $r_i$ 是使 $a_{ik}=1$ 的 $k$ 的个数，并且应用引理. 这样我们得到

$$\begin{aligned}(\text{per } A)^{n \text{ per } A} &= \prod_{i=1}^{n}(\text{per } A)^{\text{per } A} \\ &\leqslant \prod_{i=1}^{n}\left(r_i^{\text{per } A}\prod_{k,a_{ik}=1}\text{per } A_{ik}^{\text{per } A_{ik}}\right).\end{aligned} \tag{11.10}$$

令 $S$ 为{1，2，…，$n$}的所有这样的置换 $\nu$ 的集合，使 $a_{i\nu_i}=1$，$i=1$，…，$n$. 因此 $|S|=$ per $A$. 进而，$S$ 中使 $\nu_i=k$ 的 $\nu$ 的数目：当 $a_{ik}=1$ 时为 per $A_{ik}$，否则为 0. 因此，式(11.10)的右端等于

$$\prod_{\nu\in S}\left\{\left(\prod_{i=1}^{n}r_i\right)\cdot\left(\prod_{i=1}^{n}\text{per } A_{i\nu_i}\right)\right\}. \tag{11.11}$$

对每一个 $A_{i\nu_i}$ 应用归纳假设，从而有

$$(\text{per } A)^{n \text{ per} A} \leqslant \prod_{\nu \in S} \left\{ \left( \prod_{i=1}^{n} r_i \right) \cdot \prod_{i=1}^{n} \left[ \prod_{\substack{j \neq i, \\ a_{j\nu_i}=0}} (r_j!)^{1/r_j} \prod_{\substack{j \neq i, \\ a_{j\nu_i}=1}} ((r_j-1)!)^{1/(r_j-1)} \right] \right\}. \quad (11.12)$$

102

因为使 $i \neq j$ 且 $a_{j\nu_i}=0$ 的 $i$ 的个数为 $n-r_j$，而使 $i \neq j$ 且 $a_{j\nu_i}=1$ 的 $i$ 的个数为 $r_j-1$，所以我们可以用下式替换(11.12)的右端：

$$\prod_{\nu \in S} \left\{ \left( \prod_{i=1}^{n} r_i \right) \cdot \left[ \prod_{j=1}^{n} (r_j!)^{(n-r_j)/r_j} (r_j-1)! \right] \right\} = \prod_{\nu \in S} \prod_{i=1}^{n} (r_i!)^{n/r_i} = \left( \prod_{i=1}^{n} (r_i!)^{1/r_i} \right)^{n \text{ per } A},$$

从而定理得证. ■

我们现在讨论(0，1)-矩阵的一个特殊类，即每行每列都恰有 $k$ 个 1 的(0，1)-矩阵，用 $\mathcal{A}(n, k)$表示这类矩阵. 定义

$$M(n,k) := \max\{\text{per } A : A \in \mathcal{A}(n,k)\}, \quad (11.13)$$

$$m(n,k) := \min\{\text{per } A : A \in \mathcal{A}(n,k)\}. \quad (11.14)$$

通过取直和，我们有下述不等式：

$$M(n_1+n_2,k) \geqslant M(n_1,k)M(n_2,k), \quad (11.15)$$

$$m(n_1+n_2,k) \leqslant m(n_1,k)m(n_2,k). \quad (11.16)$$

由这两个不等式，应用下述的 Fekete 引理，我们还能导出两个函数.

**引理 11.6** 令 $f: \mathbb{N} \to \mathbb{N}$ 是一个函数，它满足对一切 $m$，$n \in \mathbb{N}$ 有 $f(m+n) \geqslant f(m)f(n)$，则 $\lim\limits_{n\to\infty} f(n)^{1/n}$ 存在(可能是$\infty$).

**证明** 固定 $m$ 和 $l$，$l \leqslant m$，由 $f$ 的不等式，我们可归纳地证明 $f(l+km) \geqslant f(l)[f(m)]^k$. 因此

$$\lim \inf f(l+km)^{1/(l+km)} \geqslant f(m)^{1/m},$$

103

并且由于 $l$ 有 $m$ 个可能的值，所以有

$$\lim \inf f(n)^{1/n} \geqslant f(m)^{1/m}.$$

令 $m \to \infty$，我们断定

$$\lim \inf f(n)^{1/n} \geqslant \lim \sup f(m)^{1/m},$$

然而这些取等式. ■

如果在 $f$ 的不等式中我们用$\leqslant$ 替换$\geqslant$，那么引理的断言也为真. 把这个引理应用到式(11.15)和式(11.16)，我们可定义

$$M(k) := \lim_{n\to\infty} \{M(n,k)\}^{1/n}, \quad (11.17)$$

$$m(k) := \lim_{n\to\infty} \{m(n,k)\}^{1/n}. \quad (11.18)$$

**问题 11B** 证明 $M(n, k) \geqslant k!$ 及 $M(k) \leqslant (k!)^{1/k}$. 举例说明 $M(k) \geqslant (k!)^{1/k}$，从而证明了 $M(k) = (k!)^{1/k}$.

$m(n, k)$是一个非常难处理的函数，我们的期望是基于与范德瓦尔登(Van der Waerden)

猜想有关的一个著名问题来解决，尽管在 1981 年对这个猜想给出了两个证明(事实上对这个问题已进行了近 50 年的研究了). 我们把这个猜想公式化如下，且其证明放在下一章.

**猜想** 设 $A$ 是一个 $n\times n$ 的非负元素的矩阵，其每行每列的和均为 1，那么

$$\text{per } A \geqslant n!n^{-n}. \tag{11.19}$$

在这个猜想中所讨论的矩阵，通常称为双随机矩阵. 如果 $A\in \mathcal{A}(n, k)$，那么用 $k$ 去除 $A$ 中的每一个元素，这样就得到了一个双随机矩阵. 因此，这个猜想(现已成为定理)表明 $m(k)\geqslant$ 104 $k/e$. 这是一个惊人的结果，因为问题 11B 中给出的 $M(k)$的值，当 $k\to\infty$时，趋向于 $k/e$(见评注). 这就意味着当 $n$ 很大时，对$\mathcal{A}(n, k)$中的每一个元素 $A$，$(\text{per } A)^{1/n}$的值接近 $k/e$. 长时间以来，$m(n, 3)$的最好下界是 $n+3$，即使如此，这也不易证明. 下面对这个下界的进一步改进是相当重要的也是基本的. 我们现在给出(1979)它属于 Voorhoeve 结果的证明.

**定理 11.7** $m(n, 3)\geqslant 6\cdot\left(\frac{4}{3}\right)^{n-3}$.

**证明** 令 $U_n$ 表示所有这样一些 $n\times n$ 的非负整数元素矩阵的集合，它们的每行每列的和为 3；我们令 $u(n):=\min\{\text{per } A : A\in U_n\}$. 把 $U_n$ 的每一个矩阵中的一个正元素减 1，这样得到的所有矩阵的集合记为 $V_n$，定义 $v(n):=\min\{\text{per } A : A\in V_n\}$. 我们首先证明

$$u(n)\geqslant\left\lceil\frac{3}{2}v(n)\right\rceil. \tag{11.20}$$

令 $A$ 是 $U_n$ 中的一个元素，且它的第一行为 $\boldsymbol{a}=(\alpha_1, \alpha_2, \alpha_3, 0, \cdots, 0)$，其中 $\alpha_i\geqslant 0$，$i=1, 2, 3$. 因为

$$2\boldsymbol{a}=\alpha_1(\alpha_1-1,\alpha_2,\alpha_3,0,\cdots,0)+\alpha_2(\alpha_1,\alpha_2-1,\alpha_3,0,\cdots,0)+\alpha_3(\alpha_1,\alpha_2,\alpha_3-1,0,\cdots,0),$$

那么由(11.5)，我们得到 $2u(n)\geqslant(\alpha_1+\alpha_2+\alpha_3)v(n)=3v(n)$，从而结论得证.

下面我们证明

$$v(n)\geqslant\left\lceil\frac{4}{3}v(n-1)\right\rceil. \tag{11.21}$$

我们分两种情况进行讨论. 第一种情况：$A$ 是 $V_n$ 中的一个元素，$A$ 的第一行为(1, 1, 0, …, 0)，并且去掉 $A$ 的第一行后，剩下的矩阵为形式$(\boldsymbol{c}_1, \boldsymbol{c}_2, B)$，它的列和 $\boldsymbol{c}_3:=\boldsymbol{c}_1+\boldsymbol{c}_2$ 或者为 3 或者为 4. 根据式(11.6)，我们有

$$\text{per } A=\text{per}(\boldsymbol{c}_1,B)+\text{per}(\boldsymbol{c}_2,B)=\text{per}(\boldsymbol{c}_3,B).$$

如果 $\boldsymbol{c}_3$ 的列和等于 3，则矩阵$(\boldsymbol{c}_3, B)$属于 $U_{n-1}$，从而由(11.20)得证. 如果 $\boldsymbol{c}_3$ 的列和为 4，105 那么应用和上面同样的技巧，把 $3\boldsymbol{c}_3$ 表示为 4 个向量 $\boldsymbol{d}_i$ 的线性组合，使得每一个矩阵$(\boldsymbol{d}_i, B)$属于 $V_{n-1}$，从而得到 3 per $A\geqslant 4v(n-1)$. 第二种情况：我们必须考虑 $A$ 的第一行为(2, 0, …, 0)形式. 如果去掉 $A$ 的第一行和第一列，那么得到的矩阵 $B$ 仍有两种可能性，$B$ 或者属于 $U_{n-1}$或者属于 $V_{n-1}$. 因此我们有 per $A\geqslant 2\min\{u(n-1), v(n-1)\}$，从而由(11.20)得证. 把平凡值 $v(1)=2$ 与式(11.20)和(11.21)结合起来，就可以得到定理的结论. ■

我们现在讨论更大类的 $n\times n$ 阶的非负整数元素矩阵，这些矩阵的每行每列的和均为 $k$.

我们用$\Lambda(n, k)$表示这一类矩阵，这一类矩阵中最小的积和式用$\lambda(n, k)$表示．我们仍有$\lambda(m+n, k)\leqslant\lambda(m, k)\lambda(n, k)$，并且由 Fekete 引理，可定义

$$\theta(k) := \lim_{n\to\infty}(\lambda(n,k))^{1/n}. \tag{11.22}$$

由定理 11.3 和定理 11.7，我们有$\lambda(n, 2)=2$，以及$\lambda(n, 3)\geqslant 6\cdot\left(\frac{4}{3}\right)^{n-3}$．由式(11.19)，前面我们已看到有$\lambda(n, k)\geqslant n!\left(\frac{k}{n}\right)^n$．我们还看到，积和式和不同代表系之间存在一种关系，现在我们揭示这种关系，并给予证明．

**定理 11.8** $\lambda(n, k)\leqslant k^{2n}/\binom{nk}{n}$.

**证明** 集合$\{1, 2, \cdots, nk\}$的所有有序划分为大小为$k$的一些类的总体，用$P_{n,k}$表示，则有

$$p_{n,k} := |P_{n,k}| = \frac{(nk)!}{(k!)^n}. \tag{11.23}$$

令$\mathcal{A} :=(A_1, \cdots, A_n)$是这样一个划分，则子集$A_1, \cdots, A_n$的不同代表系的个数为$k^n$个．设$\mathcal{B} :=(B_1, \cdots, B_n)$为另一个划分．我们用$s(\mathcal{A}, \mathcal{B})$表示$\mathcal{A}$和$\mathcal{B}$的公共的不同代表系的个数．定义一个$n\times n$的矩阵$A$，它的元素$a_{ij} := |A_i\cap B_j|$．证明的关键是 per $A$ 等于$\mathcal{A}$和$\mathcal{B}$的公共的不同代表系的数目．此外，由划分的定义，矩阵$A$属于$\Lambda(n, k)$．从而有

$$s(\mathcal{A},\mathcal{B}) = \text{per } A \geqslant \lambda(n,k).$$

106

如果$\mathcal{A}\in P_{n,k}$给定且$\mathcal{A}$的一个不同代表系也给定，那么存在$n!\,p_{n,k-1}$个有序划分$\mathcal{B}$，它们有相同的不同代表系．因此我们有

$$\sum_{\mathcal{B}\in P_{n,k}} s(\mathcal{A},\mathcal{B}) = k^n\cdot n!\,p_{n,k-1}.$$

把这个式子与式(11.23)和$\lambda(n, k)$的不等式结合起来，我们就得到

$$\lambda(n,k) \leqslant \frac{k^n\cdot n!\,p_{n,k-1}}{p_{n,k}} = \frac{k^{2n}}{\binom{nk}{n}}.$$ ■

这个证明是 Schrijver and Valiant(1980)给出的，他们还给出了下述推论．

**推论** $\theta(k)\leqslant\frac{(k-1)^{k-1}}{k^{k-2}}$.

**证明** 应用斯特林公式$n!\sim n^n e^{-n}(2\pi n)^{1/2}$，由上述定理就得到本推论． ■

把定理 11.7 和本推论结合起来，我们就得到$\theta(k)$的另一个值，即$\theta(3)=\frac{4}{3}$.

**问题 11C** 讨论由整数 1，2，…，64 组成的集合．首先从这个集合中去掉整数$\equiv 1 \pmod 9$，即$x_1=1$，$x_2=10$，…，$x_8=64$．然后再去掉整数$x_i+8$，其中 72 被认为是 8．这样剩下的元素集合$S$由 48 个元素组成．我们把$S$分为子集$A_1, \cdots, A_8$，其中$A_i$中的元素包含在区间$(8(i-1), 8i]$里，令$B_1, \cdots, B_8$也是$S$的一个划分且$B_i$包含整数$\equiv i \pmod 8$．那么$A_1$，…，

$A_8$ 和 $B_1$，…，$B_8$ 有多少个公共的不同代表系？

**问题 11D** 我们回到问题 5G，再考虑 $2n$ 个顶点的 3 次正则二部图．给出这个图的完美匹配数的下界．

**问题 11E** 考虑整数 1，2，…，$n$ 的一个圆排列，它的 $n$ 个子集$\{i, i+1, i+2\}(i=1, 2, \cdots, n)$有多少个不同代表系？其中整数 $i$ 为模 $n$ 的．

107

## 评注

H. Minc(1978)在他的书《Permanents》中提到，积和式这个名字虽然在 1882 年 Muir 第一次使用，但本质上应归功于 Cauchy(1812)．尽管如此，Minc 早期的一篇文章的评阅者，还是告诫他起这个名字是荒唐的．关于积和式的广泛讨论，请参阅 Minc 的书．在那本书中，人们可以发现有关解决范德瓦尔登猜想的许多理论(在写那本书时，这个猜想还未解决)．

定理 11.2 是 Ryser(1963)的工作．

关于 Minc 猜想的若干结果，请参看 Van Lint(1974)．

Fekete 引理出现在 Fekete(1923)里．关于它的另一些应用，可参阅 J. W. Moon(1968)．

把元素视为条件概率就诱导出双随机矩阵一词．但是，在概率论中还看不出积和式起什么重要的作用．

有关定理 11.7 的 $m(k)$和 $M(k)$的评论，都基于斯特林公式和相关的不等式 $n! \geq n^n e^{-n}$．应用归纳法以及$(1+n^{-1})^n$ 以 e 为极限逐渐增大的事实，很容易证明这个不等式．实际上，斯特林公式首先由棣莫弗给出，斯特林导出 $\Gamma$-函数的一个渐近级数，用以估计这个 $\Gamma$-函数．

$$\Gamma(x) = x^{x-\frac{1}{2}} e^{-x} (2\pi)^{\frac{1}{2}} e^{\theta/(12x)},$$

其中 $0<\theta<1$．($n! = \Gamma(n+1)$．)

A. Schrijver(1998)从证明不等式

$$\lambda(n,k) \geq \left(\frac{(k-1)^{k-1}}{k^{k-2}}\right)^n$$

出发，建立了定理 11.8 的推论中的相等性．

## 参考文献


L. M. Brégman (1973), Certain properties of nonnegative matrices and their permanents, *Dokl. Akad. Nauk SSSR* **211**, 27–30 (*Soviet Math. Dokl.* **14**, 945–949).

M. Fekete (1923), Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, *Math. Zeitschr.* **17**, 228–249.

J. H. van Lint (1974), *Combinatorial Theory Seminar Eindhoven University of Technology*, Lecture Notes in Mathematics **382**, Springer-Verlag.


108

H. Minc (1967), An inequality for permanents of (0,1) matrices, *J. Combinatorial Theory* **2**, 321–326.

H. Minc (1978), *Permanents*, Encyclopedia of Mathematics and its Applications, vol. 6, Addison-Wesley, reissued by Cambridge University Press.

J. W. Moon (1968), *Topics on Tournaments*, Holt, Rinehart and Winston.

H. J. Ryser (1963), *Combinatorial Mathematics*, Carus Math. Monograph **14**.

A. Schrijver (1978), A short proof of Minc's conjecture, *J. Combinatorial Theory* (A) **25**, 80–83.

A. Schrijver and W. G. Valiant (1980), On lower bounds for permanents, *Proc. Kon. Ned. Akad. v. Wetensch.* A **83**, 425–427.

A. Schrijver (1998), Counting 1-factors in regular bipartite graphs, *J. Combinatorial Theory (B)* **72**, 122–135.

M. Voorhoeve (1979), A lower bound for the permanents of certain (0,1)-matrices, *Proc. Kon. Ned. Akad. v. Wetensch.* A **82**, 83–86.

109

# 第 12 章　范德瓦尔登猜想

本章讨论规模为 $n\times\Omega_n$ 的所有双随机矩阵的集合. 用 $\Omega_n^*$ 表示这个集合中全部元素为正的矩阵构成的子集. 我们定义 $J_n:=n^{-1}J$，其中 $J$ 表示所有元素为 1 的 $n\times n$ 矩阵. 用 $\boldsymbol{j}$ 表示向量$(1, 1, \cdots, 1)^{\top}$.

在 1926 年，范德瓦尔登(B. L. van der Waerden)提出在所有双随机矩阵中，求最小的积和式问题. 很自然地认为 $\mathrm{per}J_n=n!\ n^{-n}$是最小的(已表为(11.19)). 断言

$$(A\in\Omega_n,A\neq J_n)\Rightarrow(\mathrm{per}\,A>\mathrm{per}\,J_n) \tag{12.1}$$

就成为著名的范德瓦尔登猜想(虽然他在 1969 年告诉本书的作者之一，以前没有听到过这个名字，他也没有这样的猜想). 在 1981 年，对这个猜想给出了两个不同的证明：一个是由 D. I. Falikman 在 1979 年给出的，另一个是由 G. P. Egoritsjev 在 1980 年给出的. Egoritsjev 的证明比 Falikman 的略强一些，见 Van Lint(1981)，这里将以我们的形式给出 Egoritsjev 的证明.

下面，把满足 $\mathrm{per}\,A=\min\{\mathrm{per}\,S : S\in\Omega_n\}$的矩阵 $A$ 称为**最小矩阵**. 如通常那样，将从矩阵 $A$ 中去掉第 $i$ 行和第 $j$ 列后得到的矩阵记为 $A_{ij}$. 我们常常把矩阵 $A$ 视为 $n$ 列的一个序列，并记为 $A=(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n)$. 后面将讨论 $n-1$ 阶矩阵的积和式，但我们应用 $n$ 阶矩阵的符号. 这个技巧就是把它写为 $\mathrm{per}(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_{n-1}, \boldsymbol{e}_j)$形式，其中 $\boldsymbol{e}_j$ 表示第 $j$ 个标准基向量. 如果第 $j$ 行和第 $n$ 列被去掉，那么这个积和式不改变. 我们提醒读者，按问题 5C(伯克霍夫)，集合 $\Omega_n$ 是以置换矩阵为顶点的凸集.

我们需要关于 $\Omega_n$ 中矩阵的几个基本结果. 第一个结果相当于定理 5.4.

**定理 12.1**　设 $A$ 是一个非负元素的 $n\times n$ 矩阵，那么 $\mathrm{per}\,A=0$，当且仅当 $A$ 包含一个 $s\times t$ 的零子矩阵，使得 $s+t=n+1$.

一个 $n\times n$ 的矩阵，如果它包含一个 $k\times(n-k)$的零子矩阵，则称它是**部分可分解的**. 因此，一个矩阵 $A$，如果存在置换矩阵 $P$ 和 $Q$，使得

$$PAQ=\begin{bmatrix}B & C\\ O & D\end{bmatrix},$$

则称 $A$ 是部分可分解的，其中 $B$ 和 $D$ 均是方阵. 如果一个矩阵不是部分可分解的，那么我们就称它是**完全不可分解的**. 如果 $A\in\Omega_n$ 且 $A$ 是部分可分解的，那么它在上述的表示中必有$C=O$，这是因为 $B$ 中的元素之和等于 $B$ 的列数，而 $B$ 和 $C$ 中的元素之和等于 $B$ 的行数. 因此，在这种情况下，$A$ 是 $\Omega_k$ 中的元素 $B$ 与 $\Omega_{n-k}$中的元素 $C$ 的直和，即 $B\dotplus D$.

**问题 12A**　令 $A$ 是一个 $n\times n(n\geqslant 2)$的非负元素矩阵. 证明 $A$ 是完全不可分解的，当且仅当对一切 $i$ 和 $j$，$\mathrm{per}\,A_{ij}>0$.

**问题 12B**　令 $A$ 是$n\times n$ 的非负元素矩阵，证明：如果 $A$ 是完全不可分解的，则 $AA^{\top}$ 以及 $A^{\top}A$ 都是完全不可分解的.

**定理 12.2**　最小矩阵是完全不可分解的.

**证明** 令 $A\in\Omega_n$ 是一个最小矩阵且假设 $A$ 是部分可分解的. 那么如上述, $A$ 可表示为 $A=B\dot{+}C$, 其中 $B\in\Omega_k$ 且 $C\in\Omega_{n-k}$[⊖]. 根据定理 12.1. 我们有 per $A_{k,k+1}=0$ 及 per $A_{k+1,k}=0$. 由伯克霍夫定理, 我们可以假定 $B$ 和 $C$ 的对角线上的元素都是正的. 在 $A$ 中我们用 $b_{kk}-\varepsilon$ 替换 $b_{kk}$, 用 $c_{11}-\varepsilon$ 替换 $c_{11}$, 并且在位置 $k$, $k+1$ 和 $k+1$, $k$ 上放一个 $\varepsilon$. 这样得到新的矩阵, 如果 $\varepsilon$ 充分小, 那么这个新的矩阵仍在 $\Omega_n$ 里. 这个新的矩阵的积和式等于 [111]

$$\text{per } A-\varepsilon\text{per } A_{kk}-\varepsilon\text{per } A_{k+1,k+1}+O(\varepsilon^2).$$

因为 per $A_{kk}$ 和 per $A_{k+1,k+1}$ 都是正的, 所以当 $\varepsilon$ 充分小时, 这个新的矩阵的积和式就小于 per $A$. 这个矛盾就说明了结论的正确性. ■

**推论** (i)最小矩阵的行中至少有两个正元素.

(ii)对最小矩阵中的任一元素 $a_{ij}$, 存在一个置换 $\sigma$, 使得 $\sigma(i)=j$ 且 $a_{s,\sigma(s)}>0$, $1\leqslant s\leqslant n$, $s\neq i$.

**证明** 显然(i)是平凡的, (ii)可由问题 12A 得出. ■

现在让我们看一下, 应用微积分我们能得到些什么样的结果. 在通向(12.1)的证明中, 重要的一步是下述 Marcus and Newman(1959)的惊人结果.

**定理 12.3** 如果 $A\in\Omega_n$ 是最小矩阵且 $a_{hk}>0$, 那么 per $A_{hk}=$ per $A$.

**证明** 令 $S$ 是 $\Omega_n$ 的一个子集, 它由所有这样的双随机矩阵 $X$ 组成, 使当 $a_{ij}=0$ 时, $x_{ij}=0$, 那么 $A$ 是集合 $S$ 的一个内点, 这里对某个 $m$, $S$ 是 $\mathbb{R}^m$ 的一个子集. 如果用 $Z$ 表示 $a_{ij}=0$ 的元素对$(i, j)$的集合, 那么 $S$ 可以由下述关系描述:

$$\sum_{i=1}^{n}x_{ij}=1,\quad j=1,\cdots,n;$$

$$\sum_{j=1}^{n}x_{ij}=1,\quad i=1,\cdots,n;$$

$$x_{ij}\geqslant 0,\quad i,j=1,\cdots,n;$$

$$x_{ij}=0,\quad (i,j)\in Z.$$

因为 $A$ 是一个最小矩阵, 所以积和式函数在 $S$ 的内点 $A$ 取相对最小值, 并且可以应用拉格朗日乘子来描述这种情况. 因此我们定义 [112]

$$F(X):=\text{per } X-\sum_{i=1}^{n}\lambda_i\Big(\sum_{k=1}^{n}x_{ik}-1\Big)-\sum_{j=1}^{n}\mu_j\Big(\sum_{k=1}^{n}x_{kj}-1\Big).$$

对$(i, j)\notin Z$, 我们有

$$\partial F(X)/\partial x_{ij}=\text{per } X_{ij}-\lambda_i-\mu_j.$$

由此得到 per $A_{ij}=\lambda_i+\mu_j$, 从而可以确定, 对 $1\leqslant i\leqslant n$ 有

$$\text{per } A=\sum_{j=1}^{n}a_{ij}\text{per } A_{ij}=\sum_{j=1}^{n}a_{ij}(\lambda_i+\mu_j)=\lambda_i+\sum_{j=1}^{n}a_{ij}\mu_j,\tag{12.2}$$

---

⊖ 这儿的 C 改为 D 更好些. ——译者注

类似地，对 $1\leqslant j\leqslant n$ 有

$$\operatorname{per} A=\mu_j+\sum_{i=1}^{n} a_{ij}\lambda_i. \tag{12.3}$$

我们引进向量 $\lambda=(\lambda_1,\cdots,\lambda_n)^\top$，$\mu=(\mu_1,\cdots,\mu_n)^\top$. 由(12.2)和(12.3)，我们有

$$(\operatorname{per} A)\boldsymbol{j}=\lambda+A\mu=\mu+A^\top\lambda. \tag{12.4}$$

两边用 $A^\top$ 乘，则给出

$$(\operatorname{per} A)\boldsymbol{j}=A^\top\lambda+A^\top A\mu,$$

因此 $\mu=A^\top A\mu$，类似地有 $\lambda=AA^\top\lambda$. 矩阵 $AA^\top$ 和 $A^\top A$ 都属于 $\Omega_n$，并且按定理 12.2 和问题 12B，它们有重数为 1 的特征值 1，该特征值对应的特征向量为 $\boldsymbol{j}$. 因此，$\lambda$ 和 $\mu$ 都是 $\boldsymbol{j}$ 的倍数. 由(12.4)，我们有 $\lambda_i+\mu_j=\operatorname{per} A$，并且因为 $\operatorname{per} A_{ij}=\lambda_i+\mu_j$，从而定理得证. ■

113

**注记** Marcus 和 Newman 已证明了，定理 12.3 蕴涵着 $\Omega_n^*$ 中的最小矩阵必是 $J_n$. 这个证明依赖于下述思想：令 $A$ 是 $\Omega_n$ 中的一个元素，它具有性质：对任意 $h$，$k$，$\operatorname{per} A_{hk}=\operatorname{per} A$. 如果用一个向量 $\boldsymbol{x}$，使 $\sum_{i=1}^{n} x_{ij}=1$，去替换 $A$ 的一列，那么(由(11.6)知)这个积和式的值不变. 我们把这个性质称为代换原理. 如果 $A$ 是 $\Omega_n^*$ 中的最小矩阵，那么代换原理就允许我们对 $A$ 的任意两列，用它们的平均值替代它们，并因此得到一个新的最小矩阵. 用这种方法，人们能构造一系列的最小矩阵，使它趋近于 $J_n$. 要证明最小值的唯一性，还需要一点额外的工作.

从计算出发，应用这一思想的最后一个结果，应归功于 London(1971)对定理 12.3 的下述推广.

**定理 12.4** 如果 $A\in\Omega_n$ 是最小矩阵，那么 $\operatorname{per} A_{ij}\geqslant\operatorname{per} A$ 对一切 $i$ 和 $j$ 成立.

**证明** 给定 $i$ 和 $j$，按定理 12.2 的推论(ii)，存在一个置换 $\sigma$，使得 $\sigma(i)=j$，且对任意的 $1\leqslant s\leqslant n$，$s\neq i$ 有 $a_{s,\sigma(s)}>0$. 令 $P$ 是对应的置换矩阵. 对 $0\leqslant\theta\leqslant 1$，我们定义 $f(\theta):=\operatorname{per}((1-\theta)A+\theta P)$. 因为 $A$ 是最小矩阵，所以 $f'(0)\geqslant 0$，即

$$0\leqslant\sum_{i=1}^{n}\sum_{j=1}^{n}(-a_{ij}+p_{ij})\operatorname{per} A_{ij}=-n\operatorname{per} A+\sum_{s=1}^{n}\operatorname{per} A_{s,\sigma(s)}.$$

按定理 12.3，对于 $s\neq i$，$\operatorname{per} A_{s,\sigma(s)}=\operatorname{per} A$，从而有 $\operatorname{per} A_{ij}\geqslant\operatorname{per} A$. ■

**问题 12C** 证明从定理 12.3 可推出，如果 $A\in\Omega_5^*$ 是最小矩阵，那么存在一个最小矩阵 $B\in\Omega_5^*$，它有一个 4 阶的主子矩阵 $aJ$. 然后证明 $a$ 必等于 $\frac{1}{5}$.

现在我们讨论证明范德瓦尔登猜想中的主要工具，这次我们需要线性代数. 我们将给出关于对称双线性型的一个定理的直接证明，Egoritsjev 从所谓的 Alexandroff-Fenchel 不等式出发得到了由这个定理诱导出的不等式.

114

考虑具有对称内积 $\langle\boldsymbol{x},\boldsymbol{y}\rangle=\boldsymbol{x}^\top Q\boldsymbol{y}$ 的空间 $\mathbb{R}^n$. 如果 $Q$ 有一个正特征值和 $n-1$ 个负特征值，我们就说 $\mathbb{R}^n$ 是洛伦兹(Lorentz)空间. 我们采用下述标准术语：一个非零向量 $\boldsymbol{x}$，如果内积 $\langle\boldsymbol{x},\boldsymbol{x}\rangle=0$，或 $\langle\boldsymbol{x},\boldsymbol{x}\rangle>0$，或 $\langle\boldsymbol{x},\boldsymbol{x}\rangle<0$，则分别称 $\boldsymbol{x}$ 是各向同性的，或正的，或负的.

在负特征向量生成的$(n-1)$维空间中的每一个非零向量都是负的，因此，如果 $\boldsymbol{a}$ 是正的且 $\boldsymbol{b}$ 不是 $\boldsymbol{a}$ 的标量倍数，那么由 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 生成的平面必包含一个负特征向量．因此由$\langle \boldsymbol{a}+\lambda \boldsymbol{b}, \boldsymbol{a}+\lambda \boldsymbol{b}\rangle$给出的 $\lambda$ 的二次型，必有一个正的判别式．这样我们就有下述不等式，这个不等式形式上很像柯西不等式．

**定理 12.5** *如果 $\boldsymbol{a}$ 是洛伦兹空间中的一个正向量，$\boldsymbol{b}$ 是任一向量，那么*

$$\langle \boldsymbol{a},\boldsymbol{b}\rangle^2 \geqslant \langle \boldsymbol{a},\boldsymbol{a}\rangle\langle \boldsymbol{b},\boldsymbol{b}\rangle,$$

*且等式成立当且仅当对某一个常数 $\lambda$，$\boldsymbol{b}=\lambda \boldsymbol{a}$.*

下述定义提供了内积与积和式的联系．考虑$\mathbb{R}^n$中具有正坐标的向量$\boldsymbol{a}_1$，…，$\boldsymbol{a}_{n-2}$．如通常那样，令 $\boldsymbol{e}_1$，…，$\boldsymbol{e}_n$ 是$\mathbb{R}^n$的标准基．定义$\mathbb{R}^n$上的内积为

$$\langle \boldsymbol{x},\boldsymbol{y}\rangle := \mathrm{per}(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_{n-2},\boldsymbol{x},\boldsymbol{y}), \tag{12.5}$$

即

$$\langle \boldsymbol{x},\boldsymbol{y}\rangle = \boldsymbol{x}^\top Q\boldsymbol{y},$$

其中 $Q$ 的定义为

$$q_{ij} := \mathrm{per}(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_{n-2},\boldsymbol{e}_i,\boldsymbol{e}_j). \tag{12.6}$$

注意，如果 $A$ 的列为$\boldsymbol{a}_1$，…，$\boldsymbol{a}_n$，且去掉最后两列及行 $i$ 和行 $j$，那么得到的矩阵的积和式就等于 $q_{ij}$.

[115]

**定理 12.6** *具有(12.5)定义的内积的空间$\mathbb{R}^n$是洛伦兹空间.*

**证明** 用归纳法证明．当 $n=2$ 时，$Q=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$且结论成立．假设对$\mathbb{R}^{n-1}$定理成立．第一步是证明 $Q$ 没有特征值 0．假如 $Q\boldsymbol{c}=0$，即

$$\mathrm{per}(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{n-2},\boldsymbol{c},\boldsymbol{e}_j) = 0, \quad 1\leqslant j\leqslant n. \tag{12.7}$$

去掉最后一列和第 $j$ 行，可以认为(12.7)为$\mathbb{R}^{n-1}$中向量的关系．考虑下式给出的内积：

$$\mathrm{per}(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{n-3},\boldsymbol{x},\boldsymbol{y},\boldsymbol{e}_j)_{jn}, \tag{12.8}$$

且应用归纳假设、(12.7)和定理 12.5．在(12.8)中，用 $\boldsymbol{x}=\boldsymbol{a}_{n-2}$，$\boldsymbol{y}=\boldsymbol{a}_{n-2}$替换，这样就得到一个正值，而 $\boldsymbol{x}=\boldsymbol{a}_{n-2}$，$\boldsymbol{y}=\boldsymbol{c}$ 给出 0 值，因此

$$\mathrm{per}(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{n-3},\boldsymbol{c},\boldsymbol{c},\boldsymbol{e}_j) \leqslant 0, \quad 1\leqslant j\leqslant n, \tag{12.9}$$

并且对每个 $j$ 等式成立，当且仅当对 $\boldsymbol{c}$ 的所有坐标，除 $c_j$ 外都是 0．如果用 $\boldsymbol{a}_{n-2}$的第 $j$ 个坐标乘(12.9)的左端并对 $j$ 求和，我们就得到 $\boldsymbol{c}^\top Q\boldsymbol{c}$．因此，假定 $Q\boldsymbol{c}=0$，就推出 $\boldsymbol{c}=0$.

对 $0\leqslant\theta\leqslant 1$，在(12.5)中，用 $\theta\boldsymbol{a}_i+(1-\theta)\boldsymbol{j}$ 替换 $\boldsymbol{a}_i$，这样就定义了一个 $Q_\theta$．上述表明，对区间$[0,1]$中的每一个 $\theta$，矩阵 $Q_\theta$ 都没有特征值 0．因此，正特征值的个数是常量．因为对于 $\theta=0$ 正特征值的个数为 1，而对 $\theta=1$ 正特征值的个数也是 1，这样定理就得到了证明． ■

把定理 12.5 和定理 12.6 合并起来描述为一个推论最终的结论由连续性得出.

**推论** *如果 $\boldsymbol{a}_1$，…，$\boldsymbol{a}_{n-1}$是具有正坐标的$\mathbb{R}^n$中的向量，并且 $\boldsymbol{b}\in\mathbb{R}^n$，那么*

$$(\mathrm{per}(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{n-1},\boldsymbol{b}))^2 \geqslant \mathrm{per}(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{n-1},\boldsymbol{a}_{n-1})\cdot \mathrm{per}(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{n-2},\boldsymbol{b},\boldsymbol{b}),$$

[116]

并且等式成立，当且仅当对某个常量 $\lambda$，$\boldsymbol{b}=\lambda\boldsymbol{a}_{n-1}$. 进而，若 $\boldsymbol{a}_i$ 的某些坐标为 0，这个不等式也成立，但是关于等式的结论是不可能得到的.

下面推广定理 12.3.

**定理 12.7**　如果 $A\in\Omega_n$ 是一个最小矩阵，那么对一切 $i$ 和 $j$ 有 $\operatorname{per} A_{ij}=\operatorname{per} A$.

**证明**　假定结论不对，那么按定理 12.4，存在数对 $r$，$s$，使 $\operatorname{per} A_{rs}>\operatorname{per} A$.

选取 $t$，使 $a_{rt}>0$. 考察两个因子的积 $\operatorname{per} A$，在第一个因子里我们用 $\boldsymbol{a}_t$ 代替 $\boldsymbol{a}_s$，在第二个因子里用 $\boldsymbol{a}_s$ 代替 $\boldsymbol{a}_t$. 接下来，按列 $s$ 展开第一个积和式，按列 $t$ 展开第二个积和式. 按定理 12.5 和定理 12.6 的推论，我们有

$$(\operatorname{per} A)^2\geqslant\left(\sum_{k=1}^{n}a_{kt}\operatorname{per} A_{ks}\right)\left(\sum_{k=1}^{n}a_{ks}\operatorname{per} A_{kt}\right).$$

按定理 12.4，上式右端的每一个子积和式至少等于 $\operatorname{per} A$，且 $\operatorname{per} A_{rs}>\operatorname{per} A$. 因为 $\operatorname{per} A_{rs}$ 乘一个正的 $a_{rt}$，所以上式右端大于 $(\operatorname{per} A)^2$. 这是一个矛盾. ■

我们应用代换原理如下. 取一个最小矩阵 $A$，令 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 是 $A$ 的两列，用 $\frac{1}{2}(\boldsymbol{u}+\boldsymbol{v})$ 替换 $\boldsymbol{u}$ 和 $\boldsymbol{v}$. 按定理 12.7，这个新的矩阵仍是最小矩阵.

令 $A$ 是任一个最小矩阵，$\boldsymbol{b}$ 是 $A$ 的任一列，比如是 $A$ 的最后一列，由定理 12.2 的推论(i)中，我们知道在 $A$ 的任一行中至少有两个正元素. 我们现在多次应用代换原理(如上概述)，但最后一列始终不改变. 按这种方式，我们能得到一个最小矩阵 $A'=(\boldsymbol{a}'_1, \boldsymbol{a}'_2, \cdots, \boldsymbol{a}'_{n-1}, \boldsymbol{b})$，使得 $\boldsymbol{a}'_1, \cdots, \boldsymbol{a}'_{n-1}$ 都具有正的坐标. 现在应用定理 12.6 的推论. 根据代换原理，等式必定成立. 因此对任意的 $i$，$1\leqslant i\leqslant n-1$，$\boldsymbol{b}$ 是 $\boldsymbol{a}'_i$ 的倍数. 这就意味着 $\boldsymbol{b}=n^{-1}\boldsymbol{j}$，因此 $A=n^{-1}J_n$，从而证明了范德瓦尔登猜想.

117

**定理 12.8**　蕴涵关系(12.1)成立.

## 评注

关于范德瓦尔登猜想的两个证明的综述，请参阅 Van Lint(1982). 在这篇文章中，人们还可以发现关于这个猜想的历史注记和轶事.

范德瓦尔登(B. L. van der Waerden，1903—1996)是荷兰数学家，虽然他在多个领域都发表了文章，但他在代数方面的工作是最有影响的. 他的著作《Moderne Algebra》(1931)，为几十年的发展设置了方向.

Minc 的关于积和式的书，在 1978 年以前与范德瓦尔登猜想有关的一切资料中，是最好的.

洛伦兹空间这个名字与相对论和使二次型 $x^2+y^2+z^2-t^2$ 不变的变换群有关，H. A. Lorentz 是荷兰物理学家，他的工作曾使他获得诺贝尔奖.

## 参考文献

J. H. van Lint (1981), Notes on Egoritsjev's proof of the Van der Waerden conjecture, *Linear Algebra and its Applications* **39**, 1–8.

J. H. van Lint (1982), The van der Waerden Conjecture: Two proofs in one year, *The Math. Intelligencer* **39**, 72–77.

D. London (1971), Some notes on the van der Waerden conjecture, *Linear Algebra and its Applications* **4**, 155–160.

M. Marcus and M. Newman (1959), On the minimum of the permanent of a doubly stochastic matrix, *Duke Math. J.* **26**, 61–72.

H. Minc (1978), *Permanents*, Encyclopedia of Mathematics and its Applications, vol. 6, Addison-Wesley, reissued by Cambridge University Press (1984).

B. L. van der Waerden (1926), *Jber. D. M. V.* **35**.

118

# 第 13 章　初等计数方法和斯特林数

在下述几章里将介绍一些计数方法和某些特殊的组合计数问题. 我们先从几个较常用的初等方法开始，考虑从$\{1, 2, \cdots, n\}$到$\{1, 2, \cdots, k\}$的映射，这些映射的总数为$k^n$. 在例 10.2 中，我们研究的映射是满射的情况，在定理 13.5 中我们又回到这个问题. 如果映射是单射，那么映射的数目是递降阶乘

$$(k)_n := k(k-1)\cdots(k-n+1) = k!/(k-n)!. \tag{13.1}$$

我们现在讨论一个类似的问题，被映射的 $n$ 个对象不再是不同的，而它们的像是不同的. 我们描述这个问题如下：把 $n$ 个相同的球放入标号分别为 1，2，…，$k$ 的 $k$ 个盒子里，有多少种不同的方案？利用下述技巧可以找出它的解. 设想这些球被染成蓝色，在它们要进入的盒子的前面排成一排，然后在两个相邻的盒子中间插入一个红色的球，这样就把 $n+k-1$ 个球排成一排，其中有 $k-1$ 个红球，这就描述了一种放法. 因此，问题的答案为$\binom{n+k-1}{k-1}$. 我们把它描述为下述定理.

**定理 13.1**　方程

$$x_1 + x_2 + \cdots + x_k = n \tag{13.2}$$

的非负整数解的个数为$\binom{n+k-1}{k-1}$.

119

**证明**　把 $x_i$ 看成盒子 $i$ 里的球的个数即得. ■

**推论**　如果方程(13.2)中的每一个变量 $x_i$ 都要求为正整数，则方程(13.2)有$\binom{n-1}{k-1}$个解.

**证明**　用 $y_i := x_i - 1$ 替换 $x_i$，则$\sum y_i = n-k$，然后再应用定理 13.1 即得推论. ■

**例 13.1**　与例 10.6 中遇到的问题相似，我们考虑从 1，2，…，$n$ 中选取 $r$ 个两两不相邻的整数问题，令 $x_1 < x_2 < \cdots < x_r$ 是满足要求的序列，则 $x_1 \geqslant 1$，$x_2 - x_1 \geqslant 2$，…，$x_r - x_{r-1} \geqslant 2$. 定义

$$y_1 := x_1, \quad y_i = x_i - x_{i-1} - 1, \quad 2 \leqslant i \leqslant r, \quad y_{r+1} := n - x_r + 1.$$

那么 $y_i$ 是正整数，且 $\sum_{i=1}^{r+1} y_i = n - r + 2$，因此由定理 13.1 的推论，可以看出这个问题有$\binom{n-r+1}{r}$个解.

**问题 13A**　在一个圆周上有 $n$ 个位置，我们要把整数 1，2，…，$r$ 按顺时针依次放在这些位置上，使得相继的两个数，包括数对$(r, 1)$，放在不相邻的位置上. 通过旋转得到的排列视为是相同的，那么按上述方法要把这 $r$ 个整数放到圆周的 $n$ 个位置上有多少种不同的方案？

**例 13.2**　颜色为 1 的球 $r_1$ 个，颜色为 2 的球 $r_2$ 个，…，颜色为 $k$ 的球 $r_k$ 个，把这 $n := r_1 + r_2 + \cdots + r_k$ 个球排成一排有多少种方案？如果我们把球编号为 1 到 $n$，那么有 $n!$ 种排法. 因为我们抹去了标号，所以颜色为 $i(1 \leqslant i \leqslant k)$ 的 $r_i$ 个球的任意排列都是一样的. 因此这个问题

的答案是多项式系数$\binom{n}{r_1, \cdots, r_k}$，见(2.1).

**例 13.3** 我们把集合{1，2，…，$n$}划分为若干个子集，使1个元素的子集有$b_1$个，2个元素的子集有$b_2$个，…，$k$个元素的子集有$b_k$个，其中$\sum_{i=1}^{k} ib_i=n$. 利用例13.2中已用过的相同论证对其进行讨论. 进而，相同基数的子集之间可以任意排列而不影响他们的构形. 因此，这个问题的解为

$$\frac{n!}{b_1!\cdots b_k!(1!)^{b_1}(2!)^{b_2}\cdots(k!)^{b_k}}. \tag{13.3}$$

120

很多计数问题(通常都涉及二项式系数)可以用较显而易见的方法去解，但有时会出现(困难的)计算. 解计数问题常常有一些不太显而易见的组合方法，但能得到直接答案. 我们给出几个例子.

**例 13.4** 令$A$取遍{1，2，…，$n$}的所有子集，计算$S=\sum|A|$. 因为基数为$i$的子集有$\binom{n}{i}$个，很明显，我们需计算$\sum_{i=0}^{n} i\binom{n}{i}$. 对$(1+x)^n$求导，我们有

$$\sum_{i=1}^{n} i\binom{n}{i}x^{i-1} = n(1+x)^{n-1}.$$

取$x=1$，就得到答案$S=n\cdot 2^{n-1}$. 如果我们花一点时间想一下，那么这个答案将是显而易见的！一个集合$A$和它的补合起来就包含了所有的$n$个元素，且恰有$2^{n-1}$个这样的对.

**例 13.5** 在第10章中，我们看到了关于二项式系数的某些公式，这些公式的组合证明比直接证明要容易一些. 一个熟悉的例子为

$$\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}. \tag{13.4}$$

当然，可以用$(1+x)^n(1+x)^n$中$x^n$的系数和二项式公式计算这个和式. 但(13.4)的两端只是用不同的方法计算从$n$个红球和$n$个蓝球中选取$n$个球的方式数.

**问题 13B** 证明下述二项式系数公式是式(10.6)的直接结果：

$$\binom{n+1}{a+b+1}=\sum_{k=0}^{n}\binom{k}{a}\binom{n-k}{b}.$$

按下述思路给出上式的一个组合证明：考虑集合{0，1，2，…，$n$}的$(a+b+1)$-子集，将它按增序排列，然后观察在位置$a+1$处的整数之值.

**例 13.6** 我们考虑一个更复杂一点的例子，这里用前面的知识就能得到解. 集合{1，2，…，$n$}有多少个子集序列$A_1$，…，$A_k$，使$\bigcup_{i=1}^{k} A_i=\{1, 2, \cdots, n\}$？因为要避免$j(1\leqslant j\leqslant n)$，使其不在这些$A_i$的并集里，所以我们试图利用容斥原理. 如果选取{1，2，…，$n$}中的$i$个元素，考虑所有这样的序列$A_1$，…，$A_k$，使它们不含这$i$个元素中的任何一个元素，那么这样的序列数为$(2^{n-i})^k$. 因此，由定理10.1，本问题的解为

121

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}2^{(n-i)k}=(2^k-1)^n.$$

这个答案表明了有另一种更好的方法：如果用 $k\times n$ 的(0，1)-矩阵 $A$ 表示序列 $A_1$，$A_2$，…，$A_k$，即 $A$ 的第 $i(1\leqslant i\leqslant k)$ 行为子集 $A_i$ 的特征向量，那么这些序列的条件可叙述为 $A$ 没有 0 列. 因此，这样的矩阵有 $(2^k-1)^n$ 个.

**问题 13C** 集合 $\{1, 2, \cdots, n\}$ 有多少个子集对 $(A_1, A_2)$，使得 $A_1\cap A_2=\varnothing$? 给出这个问题的两种解答方式，一种是组合解答，一种是与二项式系数有关的解答.

**问题 13D** 考虑 $\{1, 2, \cdots, n\}$ 的子集的所有有序 $k$ 元组 $\mathcal{A}=(A_1, \cdots, A_k)$ 的集 $\mathcal{S}$，确定

$$\sum_{\mathcal{A}\in\mathcal{S}} |A_1\cup A_2\cup\cdots\cup A_k|.$$

**问题 13E** 下述熟知的关系式用归纳法很容易证明：

$$\sum_{m=k}^{l}\binom{m}{k}=\binom{l+1}{k+1}.$$

有兴趣的读者可利用(10.6)给出一个更复杂的证明. 用计算 $X$-$Y$ 平面上自整数点(0，0)到整数点 $(l+1, k+1)$ 的这样一些路的数目，找出上式的一个组合证明，其中自(0，0)到 $(l+1, k+1)$ 的路按下述方式走：从(0，0)出发，若走到整点 $(x, y)$，那么从 $(x, y)$ 下一步到达的整点是 $(x+1, y)$ 或者是 $(x+1, y+1)$. 然后应用这个公式证明不等式

122

$$x_1+x_2+\cdots+x_k\leqslant n$$

的非负整数解的个数为 $\binom{n+k}{k}$. 你能用组合的方法证明这个结果吗?

为证明二项式系数之间的关系，常把 $\binom{a}{k}$ 形式地视为 $a$ 的一个多项式，即定义

$$\binom{a}{k}:=\frac{a(a-1)\cdots(a-k+1)}{k!}.$$

如果次小于等于 $k$ 的两个多项式，在变量的 $k+1$ 个值上它们相等，那么这两个多项式恒等. 下面给出一个例子.

令

$$F(a):=\sum_{k=0}^{n}\binom{a}{k}x^k y^{n-k},\quad G(a):=\sum_{k=0}^{n}\binom{n-a}{k}(-x)^k(x+y)^{n-k}.$$

由二项式定理我们知道，如果 $a$ 是区间 $[0, n]$ 中的一个整数，那么 $F(a)=(x+y)^a y^{n-a}$，再由二项式定理知 $G(a)=(x+y)^a y^{n-a}$. 因此，这两个多项式是恒等的，并且可用任意数去替换 $a$，$x$ 和 $y$，从而得到二项式系数的某些关系式. 例如，取 $y=2x$ 和 $a=2n+1$，得到

$$\sum_{k=0}^{n}\binom{2n+1}{k}2^{n-k}=\sum_{k=0}^{n}\binom{n+k}{k}3^{n-k},$$

用计数方法来得到这个关系式是相当困难的.

在许多组合问题中提出了两类数，称为第一类斯特林数和第二类斯特林数. 这些数通常由下述的公式(13.8)和(13.12)定义. 我们偏爱于组合定义.

令 $c(n, k)$ 表示 $S_n$ 中恰有 $k$ 个圈的置换 $\pi$ 的个数(这个数称为无符号的第一类斯特林数). 而且定义 $c(0, 0)=1$；若 $n\leqslant 0$ 或 $k\leqslant 0$，$(n, k)\neq(0, 0)$，定义 $c(n, k)=0$. 第一类斯特林数

定义为

$$s(n,k) := (-1)^{n-k}c(n,k). \tag{13.5}$$

123

**定理 13.2** 数 $c(n, k)$满足递推关系

$$c(n,k) = (n-1)c(n-1,k) + c(n-1,k-1). \tag{13.6}$$

**证明** 若$\pi$是$S_{n-1}$中的一个置换，且具有$k$个圈，那么存在$n-1$个位置，我们可以在这些位置上插入一个整数$n$，这样由$\pi$得到$S_n$中的具有$k$个圈的置换$\pi'$. 我们也可以在$S_{n-1}$的任意具有$k-1$个圈的置换上附加一个圈$(n)$. 这就是(13.6)的右端两项的解释. ■

**定理 13.3** 对$n\geqslant 0$，我们有

$$\sum_{k=0}^{n} c(n,k)x^k = x(x+1)\cdots(x+n-1) \tag{13.7}$$

以及

$$\sum_{k=0}^{n} s(n,k)x^k = (x)_n, \tag{13.8}$$

其中$(x)_n$的定义见(13.1).

**证明** 把(13.7)的右端写为如下形式：

$$F_n(x) = \sum_{k=0}^{n} b(n,k)x^k.$$

显然$b(0, 0)=1$. 如果$n\leqslant 0$或$k\leqslant 0$，$(n, k)\neq(0, 0)$，定义$b(n, k):=0$. 因为

$$\begin{aligned}F_n(x) &= (x+n-1)F_{n-1}(x)\\ &= \sum_{k=1}^{n} b(n-1,k-1)x^k + (n-1)\sum_{k=0}^{n-1} b(n-1,k)x^k,\end{aligned}$$

我们看到，$b(n, k)$满足的递推关系与$c(n, k)$满足的递推关系相同，即式(13.6). 因为对$n\leqslant 0$或$k\leqslant 0$，这两个数相等，所以对一切的$n$和$k$它们都相等.

124

要证明(13.8)，只要用$-x$替换$x$并应用式(13.5)即可. ■

注意，给出(13.7)式的组合证明是可能的，只要证明方程两端相同对象的计数就行了.

我们现在定义第二类斯特林数：用$P(n, k)$表示一个$n$-集划分为$k$个非空子集的所有划分的集合，那么

$$S(n,k) := |P(n,k)|. \tag{13.9}$$

仍有$S(0, 0)=1$，以及除上述定义的外，它对其余参数的取值也为0. 仍有一个容易的递推关系.

**定理 13.4** 第二类斯特林数满足关系

$$S(n,k) = kS(n-1,k) + S(n-1,k-1). \tag{13.10}$$

**证明** 其证明与定理13.3的证明几乎相同. 集合$\{1, 2, \cdots, n-1\}$的一个划分，通过它的一个子集增加元素$n$或者增加由$n$自身构成的子集就可得到$\{1, 2, \cdots, n\}$的一个划分. ■

我们定义贝尔(Bell)数$B(n)$，它是一个$n$-集的划分总数，即

$$B(n) := \sum_{k=1}^{n} S(n,k), \quad (n\geqslant 1). \tag{13.11}$$

对于第二类斯特林数，有一个类似于(13.8)的公式.

**定理 13.5** 对 $n\geqslant 0$，我们有

$$x^n=\sum_{k=0}^{n}S(n,k)(x)_k. \tag{13.12}$$

**证明** 首先注意，由式(13.9)，从一个 $n$-集到一个 $k$-集的满射的个数等于 $k!\ S(n,\ k)$(划 [125] 分的一个子集是 $k$-集中一个元素的逆像). 因此，由例 10.2，我们有

$$S(n,k)=\frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n=\frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^n. \tag{13.13}$$

令 $x$ 是一个整数，那么从 $n$-集 $N:=\{1,\ 2,\ \cdots,\ n\}$ 到 $x$-集 $\{1,\ 2,\ \cdots,\ x\}$ 有 $x^n$ 个映射. 对集合 $\{1,\ 2,\ \cdots,\ x\}$ 的任一个 $k$-子集 $Y$，从 $N$ 到 $Y$ 有 $k!\ S(n,\ k)$ 个满射，从而有

$$x^n=\sum_{k=0}^{n}\binom{x}{k}k!S(n,k)=\sum_{k=0}^{n}S(n,k)(x)_k.$$ ■

在例 10.1 中，我们看到，把一个所谓的生成函数与数的一个序列 $a_1$，$a_2$，…联系起来是很有意义的. 在第 14 章里我们将看到生成函数的许多应用，现在我们只讨论斯特林数的生成函数.

**定理 13.6** $\sum_{n\geqslant k}S(n,\ k)\frac{x^n}{n!}=\frac{1}{k!}(\mathrm{e}^x-1)^k(k\geqslant 0)$.

**证明** 令 $F_k(x)$ 表示上式左端. 由(13.10)，我们有

$$F_k'(x)=kF_k(x)+F_{k-1}(x).$$

现在用归纳法证明结论. 因为 $S(n,\ 1)=1$，所以对 $k=1$ 结论成立，并且归纳假设得到 $F_k$ 的一个微分方程，在 $S(k,\ k)=1$ 条件下，这个方程有唯一的解，即结论的右端表示式. ■

对于第一类斯特林数，要找出其生成函数要更困难一些.

**定理 13.7** $\sum_{n=k}^{\infty}s(n,\ k)\frac{z^n}{n!}=\frac{1}{k!}(\log(1+z))^k$.

**证明** 因为

[126]

$$(1+z)^x=\mathrm{e}^{x\log(1+z)}=\sum_{k=0}^{\infty}\frac{1}{k!}(\log(1+z))^kx^k,$$

定理公式的右端是 $(1+z)^x$ 展式中 $x^k$ 的系数. 另一方面，对 $|z|<1$ 我们有

$$\begin{aligned}(1+z)^x&=\sum_{n=0}^{\infty}\binom{x}{n}z^n=\sum_{n=0}^{\infty}\frac{1}{n!}(x)_nz^n\\&=\sum_{n=0}^{\infty}\frac{z^n}{n!}\sum_{r=0}^{n}s(n,r)x^r=\sum_{r=0}^{\infty}x^r\sum_{n=r}^{\infty}s(n,r)\frac{z^n}{n!}.\end{aligned}$$

这就完成了定理的证明. ■

**问题 13F** 直接证明整数 1 到 $n(n>1)$ 上所有置换中具有偶数个圈的置换个数，等于具有奇数个圈的置换个数. 再证明这个结论是定理 13.7 的一个结果.

最后，我们提一下第一类斯特林数和第二类斯特林数之间的关系：

$$\sum_{k=m}^{n}S(n,k)s(k,m)=\delta_{mn}. \tag{13.14}$$

如果在(13.12)中用(13.8)代入，则结论直接可得．因为函数 $x^n$ 和$(x)_n$($n\geqslant 0$)都构成向量空间 $\mathbb{C}[x]$的一个基，所以公式(13.14)只是基变换矩阵之间的标准关系．

**问题 13G** 证明从(13.12)式能导出 $B(n)=\frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}$.

**问题 13H** 令 $A$ 是一个 $n\times n$ 的矩阵，对一切 $i$，$j=0$，…，$n-1$，$A$ 的元素 $a_{ij}:=\binom{i}{j}$，求 $A^{-1}$.

**问题 13I** 若取 $x=\frac{1}{2}$，那么由(10.6)可得出 $\sum_{j=0}^{\infty}\binom{a+j}{j}2^{-j}=2^{a+1}$. 应用本章中的方法证明

$$\sum_{j=0}^{a}\binom{a+j}{j}2^{-j}=2^a.$$

定义

$$a_n=\sum_{j=0}^{a}\binom{a+j}{j}2^{-a-j},$$

127

替代二项式系数的基本递推关系，直接证明相同的结果，这样就得到 $a_n=\frac{1}{2}a_n+\frac{1}{2}a_{n-1}$.

**问题 13J** 如果一个集合的基数能被 3 整除，则这个集合称为好的(nice)．一个 $n$-集有多少个好的子集？

**问题 13K** 证明 $\sum_{n=1}^{\infty}S(n,n-2)x^n=\frac{x(1+2x)}{(1-x)^5}$.

## 评注

第一类斯特林数和第二类斯特林数出现在数学的许多领域里．例如，在许多插值公式以及有限差分计算中，它们都起着重要作用．在一些书中的数学函数表里，都有这些数的表．

在后面的第 37 章里，这些数还会出现．

斯特林(James Stirling，1692—1770)是苏格兰数学家，毕业于牛津大学．他在威尼斯和伦敦教过数学，但在 43 岁时，他改行从事商业活动．

128

# 第 14 章　递推关系和生成函数

许多组合计数问题，当它的解 $a_n$ 依赖于参数 $n$ 时，可以通过找出 $a_n$ 的一个递推关系，然后解这个递推关系求其解. 有时可以引进一个普通生成函数

$$f(x) := \sum_{n\geqslant 0} a_n x^n,$$

或者指数生成函数

$$f(x) := \sum_{n\geqslant 0} a_n \frac{x^n}{n!},$$

并且应用递推关系找出 $f(x)$的方程或微分方程，然后解这个方程求出递推关系的解. 我们将给出这些方法的几个例子.

**例 14.1**　作为入门，再看一下例 10.1. 令 $\pi$ 是$\{1, 2, \cdots, n+1\}$的一个更列排列，对 $\pi(n+1)$有 $n$ 种选择. 若 $\pi(n+1)=i$ 且 $\pi(i)=n+1$，那么 $\pi$ 也是集合$\{1, 2, \cdots, n\}\setminus\{i\}$上的一个更列排列. 如果 $\pi(n+1)=i$ 且 $\pi(i)\neq n+1=\pi(j)$，那么用 $i$ 替换 $\pi(j)$，这样得到$\{1, 2, \cdots, n\}$集合上的一个更列排列. 因此

$$d_{n+1} = n(d_n + d_{n-1}), \tag{14.1}$$

这是(10.3)的一个直接推论. 设 $D(x)$是序列 $d_0=1$，$d_1=0$，$d_2$，… 的指数生成函数. 由(14.1)我们立刻得到

129

$$(1-x)D'(x) = xD(x),$$

并且由此可得 $D(x)=\mathrm{e}^{-x}/(1-x)$及(10.2).

在许多情况中，我们把生成函数只用做一个簿记装置，并且加法和乘法运算(甚至下面将看到的代换和导数)被形式地解释. 给出形式的级数(作为代数对象)的完全严格的理论是可能的，在附录 2 里我们对这一理论作了介绍. 在大多数情况下，检查运算的合理性直观上是显而易见且容易的. 如果使用的级数实际上是收敛的，那么与例 14.1 中一样，我们可以利用级数的所有合适的知识. 这里给出另一个基本例子.

**例 14.2**　我们设想有编号 1 到 $k$ 的 $k$ 个盒子，并且盒子 $i$ 装有 $r_i$ 个球，$1\leqslant i\leqslant k$. 列出所有可能构形的形式簿记装置是指定一个构形对应于下述乘积中的一项 $x_1^{r_1}x_1^{r_2}\cdots x_k^{r_k}$：

$$(1+x_1+x_1^2+\cdots)(1+x_2+x_2^2+\cdots)\cdots(1+x_k+x_k^2+\cdots).$$

我们把所有涉及恰好 $n$ 个球的项集中起来，令对一切 $i$，$x=x_i$，那么这些项都等于 $x^n$. 因此，就得到了把 $n$ 个球放入 $k$ 个不同盒子里的方式数是$(1-x)^{-k}$展式中 $x^n$ 的系数，并根据式(10.6)，这个系数为$\binom{k-1+n}{n}$，这就给出了定理 13.1 的第二个证明.

在许多情况中，一个有意义的组合问题能引出一个具有常系数的线性递推关系，而线性递推关系用标准方法很易求解.

**例 14.3**　我们讨论在 $X$-$Y$ 平面上从(0, 0)点出发的长为 $n$ 的路的数目，这些路必须满足下述规则：假如到达点$(x, y)$，那么从$(x, y)$出发下一步有三种可能，即 $R:(x, y)\to(x+1, y)$，$L:(x, y)\to(x-1, y)$，$U:(x, y)\to(x, y+1)$(即向右、向左或向上走一格). 还

要求 $R$ 和 $L$ 两步不能相邻，即向右走一格，下一步不能向左走；而向左走一格，下一步不能向右走. 令 $a_n$ 表示这样的路的总数. 如果用 $b_n$ 表示这些路中从(0, 0)出发第一步是向上走一格的路的数目，那么 $b_n=a_{n-1}$，进而显然有 $b_{n+m}\geqslant b_nb_m$ 及 $b_n\leqslant 3^{n-1}$. 因此，按 Fekete 引理，即引理 11.6，$\lim\limits_{n\to\infty}b_n^{1/n}$ 存在且最多为 3. 注意到 $a_0=1$ 及 $a_1=3$. 根据最后一步或两步的方向，我们把所有长为 $n$ 的路之集合分为 $n$ 个子集. 显然，最后一步是 $U$(即向上)的路有 $a_{n-1}$条. 如果长为 $n-1$ 的路其最后一步是 $L$ 或 $R$，那么再接一个 $L$ 或 $R$ 就得到长为 $n$ 的路；若长为 $n-1$ 的路其最后一步是 $U$，则再接一个 $L$ 也得一条长为 $n$ 的路. 按这种方法我们得到长为 $n$ 且最后两步为 $LL$，$RR$ 或 $UL$ 的路的数目为 $a_{n-1}$. 剩下的是最后两步为 $UR$ 的长为 $n$ 的路之数目，显然这样的路有 $a_{n-2}$条. 因此有 [130]

$$a_n = 2a_{n-1}+a_{n-2} \quad (n\geqslant 2).$$

令 $f(x)=\sum\limits_{n=0}^{\infty}a_nx^n$，那么由递推关系可得

$$f(x)=1+3x+2x(f(x)-1)+x^2f(x),$$

即

$$f(x)=\frac{1+x}{1-2x-x^2}=\frac{\frac{1}{2}\alpha}{1-\alpha x}+\frac{\frac{1}{2}\beta}{1-\beta x},$$

其中 $\alpha=1+\sqrt{2}$，$\beta=1-\sqrt{2}$，因此

$$a_n=\frac{1}{2}(\alpha^{n+1}+\beta^{n+1}),$$

并且我们发现 $\lim\limits_{n\to\infty}a_n^{1/n}=1+\sqrt{2}$.

**问题 14A** (i)设长为 $n$ 且不含两个 0 相邻的(0, 1)-序列的个数为 $a_n$，求 $a_n$.

(ii)令 $b_n$ 表示这样的长为 $n$ 的(0, 1)-序列的个数，这些序列中没有两个 1 相邻，并且 0 只能以相继的两个 0 或 3 个 0 出现，包括序列的开头和结尾也是这样. 证明存在某个 $c$，使 $b_n^{1/n}\to c$，并求 $c$ 的近似值.

**例 14.4** 令 $a(r, n)$表示例 13.1 中问题的解的个数，其中 $0\leqslant r\leqslant n$，$a(0, 0)=1$. 我们把所有可能的序列分为两个子集：一个是 $x_1=1$ 的序列的集合，一个是 $x_1>1$ 的序列的集合. 第一个子集中的序列数显然为 $a(r-1, n-2)$；而第二个子集中的序列数为 $a(r, n-1)$. 因此

$$a(r,n)=a(r,n-1)+a(r-1,n-2) \quad (n>1). \tag{14.2}$$

[131]

由这个递推关系，我们可以用归纳法证明 $a(r, n)=\binom{n-r+1}{r}$. 若用生成函数证明要更困难些. 试用

$$f(x,y):=\sum_{n=0}^{\infty}\sum_{r=0}^{\infty}a(r,n)x^ny^r$$

证明之. 由(14.2)，我们有

$$f(x,y)=1+x+xy+x(-1+f(x,y))+x^2yf(x,y),$$

即

$$f(x,y)=\frac{1+xy}{1-x-x^2y}=\frac{1}{1-x}+\sum_{a=1}^{\infty}\frac{x^{2a-1}y^a}{(1-x)^{a+1}}.$$

用(10.6)式替换$(1-x)^{-a-1}$，即得$a(r, n)$的表示式.

像我们在例 14.3(和问题 14A) 中已看到的，常系数线性递推关系诱导出一个有理函数作为生成函数(且反之亦然). 的确，如果 $a_n=\sum_{k=1}^{l}\alpha_k a_{n-k}(n>l)$，并且 $f(x)=\sum_{n=0}^{\infty}a_n x^n$，那么 $\left(1-\sum_{k=1}^{l}\alpha_k x^k\right)f(x)$ 是一个幂级数，并且当 $n>l$ 时，$x^n$ 的系数为 0.

下述 Klarner(1967)的例子显示了线性递推关系的一个有趣情形，这个递推关系是借助于生成函数发现的，而没有明显的组合方法去适应它.

**例 14.5** 观察图 14.1 中的平面构形，这样的构形称为多方块牌(polyomino)，它由若干层组成，每一层由若干个相继的小方格组成，而相继的两层由上下两层相互对齐的一串小方格相邻. (更精确地，我们研究水平凸多方块牌).

132

图 14.1

令 $a_n$ 表示具有 $n$ 个方格的多方块牌的个数，定义 $f(x):=\sum_{n=1}^{\infty}a_n x^n$. 为了求出 $f$，我们引进数 $a(m,n)$，它表示 $n$ 个方格的所有多方块牌中，其底层具有 $m$ 个方格的多方块牌的个数. 若 $m>n$，定义 $a(m,n):=0$. 显然

$$a(m,n)=\sum_{l=1}^{\infty}(m+l-1)a(l,n-m). \tag{14.3}$$

我们定义

$$F(x,y):=\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}a(m,n)x^n y^m. \tag{14.4}$$

那么 $f(x)=F(x, 1)$. 因为后面这个级数还要出现，定义

$$g(x):=\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}ma(m,n)x^n.$$

我们记

$$g(x)=\left(\frac{\partial F}{\partial y}\right)_{y=1}. \tag{14.5}$$

即使我们有形式幂级数理论，也可以证明(14.4)右端在足够大的定义域内收敛. 这就给我们机会去找出粗略估计 $a_n$ 的一个快速方法. 如图 14.1 一样，给多方块牌中的方格编号. 对每一个方格有一个(0, 1)-四元组$(x_0, x_1, x_2, x_3)$与其对应. 其中 $x_0=1$ 表示在多方块牌中这个方格的下方有一个方格；$x_1=1$ 表示这个方格的左方有一个方格；$x_2=1$ 意味着这个方格的上方有一个方格；$x_3=1$ 表示这个方格的右方有一个方格. 例如在图 14.1 中，方格 1 对应的四元组为(0, 0, 1, 1). 四元组序列唯一地确定了多方块牌. (例如，第 5 个四元组是这个序列中第一个以 0 为末元的四元组，这就表示 $m=5$，…). 这表明了 $a_n\leqslant 15^n$. 由此及(14.3)，我们有 $a(m, n)\leqslant n\cdot 15^{n-m}$，这足以说明(14.5)的合理性. 将(14.3)代入(14.4)，直接计算可得

133

$$F(x,y)=\frac{xy}{1-xy}+\frac{(xy)^2}{(1-xy)^2}f(x)+\frac{xy}{1-xy}g(x). \tag{14.6}$$

(14.6)式两端对 $y$ 求导，当取 $y=1$(应用(14.5))时，就可得到

$$g(x)=\frac{x}{(1-x)^2}+\frac{2x^2}{(1-x)^3}f(x)+\frac{x}{(1-x)^2}g(x). \tag{14.7}$$

从(14.7)中解出 $g(x)$，把 $g(x)$的表示式代入(14.6)中，然后取 $y=1$，从而得到

$$f(x)=\frac{x(1-x)^3}{1-5x+7x^2-4x^3}. \tag{14.8}$$

由(14.8)，可看出 $a_n$ 满足递推关系

$$a_n=5a_{n-1}-7a_{n-2}+4a_{n-3}\quad(n\geqslant 5). \tag{14.9}$$

正如上述所说过的，人们完全不清楚如何能给出一个直接的证明，然而我们已经间接地做到了.

**注记** 从(14.9)式中，我们有 $\lim_{n\to\infty}a_n^{1/n}=\theta$，其中 $\theta$ 是多项式 $x^3-5x^2+7x-4$ 的绝对值最大的零点($\theta\approx 3.2$).

由下述例子可导出有限域理论中的一个重要结果，这个例子是例 14.2 的思想推广与形式幂级数方法的结合. 读者应相信，下述对数运算不应用收敛性也是正确的.

**例 14.6** 计算 $q$ 个元素域上的不可约 $n$ 次多项式的个数.

把 $q$ 个元素域上次至少是 1 的所有不可约的首一多项式编号为

$$f_1(x),f_2(x),f_3(x),\cdots,$$

134

使它们的次分别为 $d_1$，$d_2$，$d_3$，…. 令 $N_d$ 表示次 $d$ 的数目，其中 $d=1$，2，3….

对任一个非负整数序列 $i_1$，$i_2$，$i_3$，…(允许有有限个 0)，我们得到首一多项式

$$f(x)=(f_1(x))^{i_1}(f_2(x))^{i_2}(f_3(x))^{i_3}\cdots,$$

它的次为 $n=i_1d_1+i_2d_2+i_3d_3+\cdots$. 由因子分解的唯一性，按这种方式，每个 $n$ 次首一多项式恰出现一次. 重复这一过程，那么 $n$ 次首一多项式与满足 $n=i_1d_1+i_2d_2+i_3d_3+\cdots$的非负整数序列 $i_1$，$i_2$，…之间就存在 1-1 对应.

当然，$n$ 次首一多项式的个数为 $q^n$，即下式中 $x^n$ 的系数：

$$\frac{1}{1-qx}=1+qx+(qx)^2+(qx)^3+\cdots.$$

显然(参考例 14.2)，使 $n=i_1d_1+i_2d_2+\cdots$的序列 $i_1$，$i_2$，…的数目是下述形式幂级数中 $x^n$ 的系数：

$$(1+x^{d_1}+x^{2d_1}+x^{3d_1}+\cdots)(1+x^{d_2}+x^{2d_2}+x^{3d_2}+\cdots)\cdots.$$

因此，我们有

$$\frac{1}{1-qx}=\prod_{i=1}^{\infty}\frac{1}{1-x^{d_i}}=\prod_{d=1}^{\infty}\left(\frac{1}{1-x^d}\right)^{N_d}.$$

对这个方程两端取对数，并利用 $\log\frac{1}{1-z}=z+\frac{1}{2}z^2+\frac{1}{3}z^3+\cdots$，有

$$\sum_{n=1}^{\infty}\frac{(qx)^n}{n}=\sum_{d=1}^{\infty}N_d\sum_{j=1}^{\infty}\frac{x^{jd}}{j}.$$

然后比较此式两端 $x^n$ 的系数，得

$$\frac{q^n}{n}=\sum_{d\mid n}N_d\frac{1}{n/d},$$

135

即

$$q^n = \sum_{d|n} dN_d.$$

最后这个方程就是我们所要求的. 我们由因子分解的唯一性组合地导出了此式，但注意，实际上可以用 $q$ 个元素域上 $x^{q^n}-x$ 的因子分解的术语给它一个精彩的解释. 应用默比乌斯反演(见定理 10.4)，我们得到下述定理.

**定理 14.1** 设 $q$ 是素数幂，$q$ 个元素域上 $n$ 次不可约的首一多项式的个数为

$$N_n = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d.$$

注意，定理 14.1 的一个直接结果是 $N_d>0$，即对每一个 $d$，都存在不可约的 $d$ 次多项式. 这个结果直接导出对每一个素数 $p$ 都存在 $p^d$ 个元素域的证明，而不是通常采用证明素数阶域的代数封闭性的手段.

* * *

现在我们讨论具有相同解的一大类计数问题. 因为 Catalan(1838)研究过例 14.7，所以这类计数问题称为卡塔兰(Catalan)族. 实际上，von Segner 和欧拉(Euler)在 18 世纪研究过一个等价的问题，这个问题是下述例 14.9 中的问题 3. 我们用 $u_n$ 表示这些问题的解，$u_n=\frac{1}{n}\binom{2n-2}{n-1}$，这些数称为卡塔兰数.

**例 14.7** 我们有一个集合 $S$ 连同一个非结合的积运算. 对于 $x_i\in S$，表示式 $x_1x_2\cdots x_n$ 不表示任何意义，必须用括号来表示运算执行的顺序. 令 $u_n$ 表示对 $n$ 个因子 $x_i$，括号设置的方式数. 例如，$u_4=\frac{1}{4}\binom{6}{3}=5$ 对应于积$(a(b(cd)))$，$(a((bc)d))$，$((ab)(cd))$，$((a(bc))d)$ 和 $(((ab)c)d)$. 外括号里每一个积含两个表示式，第一个是 $m$ 个因子的积，第二个是 $n-m$ 个因子的积，其中 $1\leqslant m\leqslant n-1$. 由此得到 $u_n$ 的递推式：

136

$$u_n = \sum_{m=1}^{n-1} u_m u_{n-m} \quad (n \geqslant 2). \tag{14.10}$$

由(14.10)及 $u_1=1$，可得生成函数 $f(x):=\sum_{n=1}^{\infty}u_n x^n$ 满足方程

$$f(x) = x + \sum_{n=2}^{\infty}\left(\sum_{m=1}^{n-1}u_m u_{n-m}\right)x^n = x + (f(x))^2. \tag{14.11}$$

解这个二次方程，且考虑到 $f(0)=0$，则有

$$f(x) = \frac{1-\sqrt{1-4x}}{2}.$$

由二项式级数，我们有

$$u_n = \frac{1}{n}\binom{2n-2}{n-1}. \tag{14.12}$$

上述执行的运算，作为幂级数的形式运算是合理的，并且二项式级数也可以形式地处理，而不涉及收敛性. 如果感到这种方法不容易，那么有两种补救方法. 第一种方法是找出一个解，然

后用(14.10)和归纳法证明其正确性. 如果人们真想证明这个生成函数是由一个收敛幂级数所确定的，那么应用这个计算结果给 $u_n$ 一个粗略估计，并应用(14.11)证明这个估计的正确性，然后证明这个级数是收敛的. 例如，我们试验 $u_n \leqslant c^{n-1}/n^2$. 对 $n=1$ 和任意正数 $c$ 这个不等式是成立的. 对于 $n=2$，当 $c \geqslant 4$ 时，这个不等式也成立. 假设对 $m \leqslant n-1$ 存在常量 $c$ 使 $u_m \leqslant \frac{1}{m^2}c^{m-1}$ 成立. 那么应用(14.11)且当 $c \geqslant \frac{4}{3}\pi^2$ 时，有

$$u_n \leqslant c^{n-2}\sum_{m=1}^{n-1}\frac{1}{m^2(n-m)^2} \leqslant c^{n-2}\frac{2}{(n/2)^2}\sum_{m=1}^{\infty}\frac{1}{m^2} < \frac{c^{n-1}}{n^2}.$$

[137]

因此，$\sum_{n=1}^{\infty} u_n x^n$ 的收敛半径大于 0.

**注记** 公式(14.10)表明 $u_n \geqslant u_m u_{n-m}$，那么由 Fekete 引理可推出极限 $\lim_{n\to\infty} u_n^{1/n}$ 存在. 实际上，(14.12)就表明了这个极限为 4.

前面已说过，卡塔兰数在一些组合计数问题中经常出现. 这就导致组合地证明其他一些问题的方法，即在其他问题的计数对象与例 14.7 中的计数对象之间，建立起一一对应的关系. 在例 14.9 中我们将讨论这样一些问题，我们先看另一个有名的计数问题，它的解也是卡塔兰数.

**例 14.8** 讨论在 $X$-$Y$ 平面上的行走问题，每一步或向右上：$U:(x, y)\to(x+1, y+1)$，或向右下：$D:(x, y)\to(x+1, y-1)$，那么从(0, 0)出发走到点$(2n, 0)$在不允许穿过 $X$-轴的情况下，有多少条行走路线？解这个问题要用到一个优美的方法，称为 André 反射原理(1887). 在图 14.2 中，考虑上半平面中的两个点 $A$ 和 $B$ 及 $A$ 和 $B$ 之间的一条路，这条路可能与 $X$-轴相遇或穿过 $X$-轴.

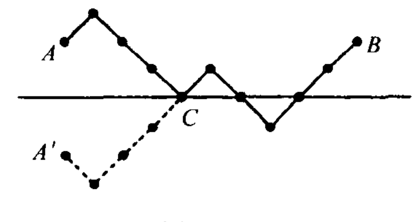


图 14.2

设从 $A$ 到 $B$ 这条路上与 $X$-轴相交的第一个点为 $C$，那么把从 $A$ 到 $C$ 这段作关于 $X$-轴的反射，就得到从 $A$ 的反射点 $A'$到 $B$ 的一条路. 这样我们就在从 $A'$到 $B$ 的路以及 $A$ 到 $B$ 的路中与 $X$-轴相遇或穿过 $X$-轴的路之间建立了一一对应.

由此可得，若 $A=(0, k)$，$B=(n, m)$，那么从 $A$ 到 $B$ 且与 $X$-轴相遇或穿过 $X$-轴的路有 $\binom{n}{l_1}$条，其中 $2l_1 := n-k-m$. 从而从 $A$ 到 $B$ 不与 $X$-轴相遇的路有 $\binom{n}{l_2}-\binom{n}{l_1}$条，这是因为从 $A$ 到 $B$ 的路共有 $\binom{n}{l_2}$条，其中 $2l_2=n-m+k$. 在上半平面里，从点(0, 0)到$(2n, 0)$且与这两个点之间的 $X$-轴不相遇的每一条路，其走向都是从(0, 0)到$(1, 1) := A$，从 $A$ 到 $B := (2n-1, 1)$是与 $X$-轴不交的一段路，然后再从$(2n-1, 1)$到$(2n, 0)$. 按上述论证，这样的路的数目为 $u_n$. 如果允许这些路与 $X$-轴相遇但不允许穿过 $X$-轴，那么这样的路有 $u_{n+1}$条.

[138]

注意，上半平面中从(0, 0)到$(2n, 0)$且与这两个点之间不相遇的路之数目，等于满足下述条件的(0, 1)-序列$(x_1, x_2, \cdots, x_{2n})$的数目：

$$x_1+x_2+\cdots+x_j\begin{cases}<\dfrac{1}{2}j & 1\leqslant j\leqslant 2n-1,\\ =n & j=2n.\end{cases} \tag{14.13}$$

这样的序列与(0，0)到(2$n$，0)的对应是：序列中的 1 对应于向右下走一步，即一步 $D$，0 表示一步 $u$.

我们现在组合地证明几个答案为卡塔兰数的计数问题.

**例 14.9** 思考下面的三个问题.

问题 1. 画在平面上的一棵树称为平面树，$n$ 个顶点的有根平面树有多少棵？根次为 1 的平面树(称为种植平面树)有多少棵？

问题 2. 一棵种植树，如果每一个顶点的次为 1 或 3，则称它为三价或二分树，具有 $n$ 个顶点次为 1 的种植二分平面树有多少棵？

问题 3. 一个凸 $n$ 边形，用它的 $n-3$ 条不相交的对角线将其划分为三角形，那么将凸 $n$ 边形划分为三角形有多少种不同的方案？

139 我们首先证明问题 2 和例 14.7 之间的对应.

为此，只要看一下图 14.3 就足够了.

由此知问题 2 的解为 $u_{n-1}$.

问题 1. 和例 14.8 之间的对应由图 14.4 也可看出.

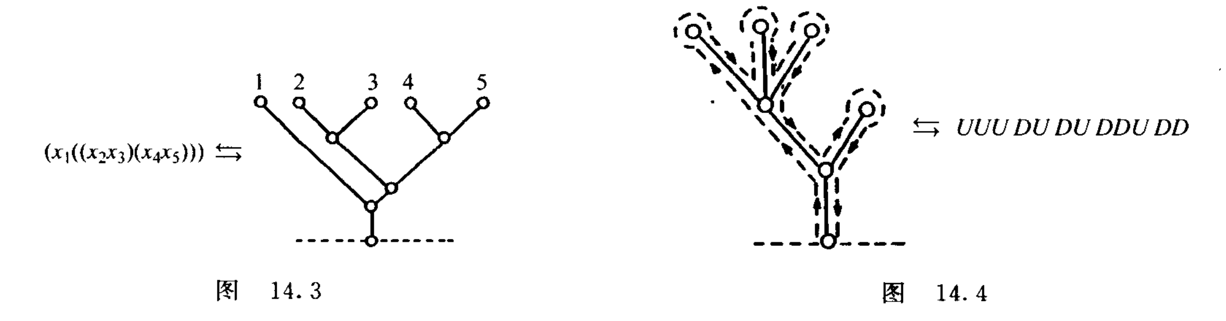



图 14.3　　图 14.4

这个图中的树可以用一条围绕这棵树转一圈的步路表示，如图中虚线所示. 这个步路可以用向上走一步 $U$ 和向下走一步 $D$ 的序列表示. 这样就产生了 12 步的序列. 用 0 表示 $U$，用 1 表示 $D$. 这就产生一个序列满足(14.13)，从而说明问题 1 的解也是 $u_{n-1}$.

最后，我们证明问题 3 和问题 2 之间的对应. 考虑一个被划分为三角形的凸 $n$ 边形和它的一条特殊的边. 我们构造一棵树，如图 14.5 所示.

140

这棵树是二分树，次为 1 的顶点对应于 $n$ 边形的边，次为 3 的顶点对应于三角形. 这棵树被种植在对应于特殊边的顶点上. 因此，这个问题的解仍是 $u_{n-1}$.

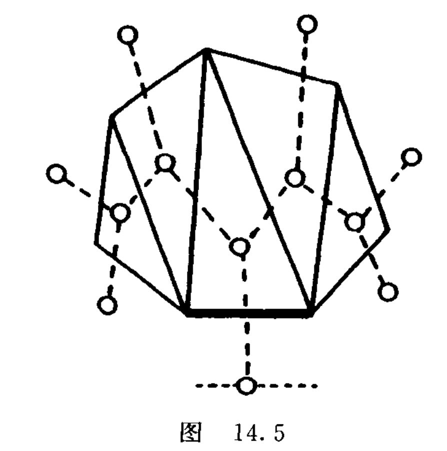


图 14.5

**问题 14B** 用一个图描述问题 1 的图和问题 2 的图之间的对应.

**问题 14C** 直接找一个从问题 3 的 $n$ 边形到例 14.7 的积的一一对应.

我们现在看另一些问题，对这些问题而言，指数生成函数显得更有用. 我们将给出较系统的讨论，这种方法较完整的讨论见 A. Joyal(1981).

令 $M$ 表示组合结构的一种类型，例如树、多边形、集合(均匀结构)、置换等. 令 $m_k$ 表示给出标记的 $k$-集这样一个结构的方式数. 对不同的情况，将规定 $m_0=0$ 或 $m_0=1$. 我们用大写字母表示结构，小写字母表示计数序列. 我们定义

$$M(x) := \sum_{k=0}^{\infty} m_k \frac{x^k}{k!}. \tag{14.14}$$

因此，若 $T$ 表示(标号的)结构树，那么由定理 2.1 知 [141]

$$T(x) = \sum_{k=0}^{\infty} k^{k-2} \frac{x^k}{k!}.$$

如果 $S$ 表示均匀结构(集合)，那么对一切 $k$，有 $s_k=1$，因此 $S(x)=e^x$. 如果 $C$ 表示“定向回路”，那么从顶点 1 开始显然有 $(k-1)!$ 个不同的定向回路. 因此，$C(x)=-\log(1-x)$.

我们考虑把一个标号的 $n$-集划分为两部分，一部分具有 $A$ 型结构，另一部分具有 $B$ 型结构的方式数. 容易看出，这种做法的方式数为 $\sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}$. 如果称它为 $A\cdot B$ 型结构，那么

$$(A\cdot B)(x) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}\right)\frac{x^n}{n!} = A(x)\cdot B(x). \tag{14.15}$$

读者应小心对待(14.15)的结果，这个结果只有在下述情况下才是正确的，即由复合结构能唯一地找出导致这个结构划分的两部分. 例如，若 $A$ 和 $B$ 是相同的，那么这个结果显然是错误的.

**例 14.10** 我们再次讨论更列排列问题，称更列排列为 $D$ 型结构，令 $\Pi$ 表示“置换”结构. 显然有 $\Pi(x)=(1-x)^{-1}$. 任一个置换由两部分组成，一部分是不动点(把它们视为一个集合)，另一部分是更列的点. 因此，由(14.15)有

$$(1-x)^{-1} = D(x)\cdot S(x), \quad 即\ D(x) = e^{-x}(1-x)^{-1},$$

这就是前面例 10.1 中的结果.

**例 14.11** 将一个标号的 $n$-集分割为一些元素对($=P$)和一些单一元素集($=S$)，有多少种不同的方案? 首先观察，若把 $2k$ 个点分割为元素对的情况，此时必须选取一个元素 $x_1$ 与点 1 组成对，然后剩余的 $2k-2$ 个点分割为元素对. 因此我们有 $p_{2k}=(2k-1)!!$，并且有

$$P(x) = \sum_{k=0}^{\infty}(2k-1)!!\frac{x^{2k}}{(2k)!} = \exp\left(\frac{1}{2}x^2\right).$$ [142]

由此可得

$$(P\cdot S)(x) = \exp\left(x+\frac{1}{2}x^2\right). \tag{14.16}$$

现在我们试着用递推关系来给出这一结果. 用 $B$ 表示 $P\cdot S$ 结构. 在集合$\{1, 2, \cdots, n\}$中，$n$ 可以是分割中的单一元素集或者它与某个元素 $x(1\leqslant x\leqslant n-1)$组成元素对$\{x, n\}$，因此

$$b_n = b_{n-1} + (n-1)b_{n-2} \quad (n \geqslant 1).$$

由这个递推关系得到

$$B'(x) = (1+x)B(x),$$

因为 $B(0)=1$，我们就得出它的解就是(14.16).

在例 14.15 中我们又回到了例 14.11 的递推关系.

**问题 14D** 考虑下述一些结构：$M_0$ ：=一个集合到自身的映射且没有不动点，$M_1$ ：=一个集合到自身的映射且恰有一个不动点，$A$ ：=树形图. 找出 $M_0(x)$，$M_1(x)$和 $A(x)$之间的关系，并检验前几项看是否正确.

下面讨论更难一点的问题. 把一个 $n$-集划分为若干部分，并使每一部分具有结构 $N$，其中 $n_0=0$. 我们断定：这个复合结构的指数生成函数为 $\exp(N(x))$. 一个简单的例子是，当 $N$ 为均匀结构时(通常 $n_0=0$)，$N(x)=\mathrm{e}^x-1$. 此时就是上述情形. 复合结构当然是"划分"，由定理 13.6 知，其指数生成函数为

$$\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}S(n,k)\right)\frac{x^n}{n!} = \sum_{k=0}^{\infty}\frac{(\mathrm{e}^x-1)^k}{k!} = \exp(\mathrm{e}^x-1) = \exp(N(x)).$$

我们把这种方法描述为一个定理.

**定理 14.2** 如果复合结构 $S(N)$是由分割一个集合为几部分，而每一部分是 $N$ 型结构得到的，那么

143

$$S(N)(x) = \exp(N(x)).$$

**证明** 把(13.3)略加推广，我们就看出，若一个 $n$-集的划分是由 $b_1$ 个部分均含 1 个元素，$b_2$ 个部分均含 2 个元素，…，$b_k$ 个部分均含 $k$ 个元素组成，其中 $b_1+2b_2+\cdots+kb_k=n$，那么构造一个复合结构的方式数为

$$\left(\frac{n_1}{1!}\right)^{b_1}\cdots\left(\frac{n_k}{k!}\right)^{b_k}\cdot\frac{n!}{b_1!\cdots b_k!}.$$

这个数除以 $n!$ 就得到指数生成函数中 $x^n$ 的系数. 若 $b_1+b_2+\cdots+b_k=m$，则有同样的结果，即

$$\frac{1}{m!}\binom{m}{b_1,\cdots,b_k}\left(n_1\frac{x}{1!}\right)^{b_1}\cdots\left(n_k\frac{x^k}{k!}\right)^{b_k}.$$

定理得证. ■

事实上，不难看出这个定理是一个更一般方法的特殊情况. 解释前述情况如下，在点的 $k$-集上有一个均匀结构，我们用某一个 $N$ 型结构代替每一个点. 这样导出的构形就是我们刚讨论过的复合结构的一个元素，如果第一个结构不是均匀的，比如是 $R$ 型结构，那么用相同的论证可得这个复合结构的指数生成函数为 $R(N(x))$. 有时我们把这个过程称为 $N$ 代入 $R$，并且有趣的是对生成函数也可以这样做.

**例 14.12** 如果把定向圈的结构代入均匀结构，那么考虑由 $n$-集划分为定向圈构成的复合结构，即具有 $\pi_0=1$ 的结构 $\Pi$，因此我们必定有 $\Pi(x)=\exp(C(x))$，且 $\Pi(x)=(1-x)^{-1}$和 $C(x)=-\log(1-x)$.

**例 14.13** 让我们再看一下图 2.2，在顶点 1 和 21 上增加环. 那么这个图描述为 $n$-集到自身的映射(这里 $n=21$). 也可以解释它是结构 $\Pi$ 的一个元素，即(1)(4，5，3)(7)(20，12)(21)中的每一个点用以该点为根的树形图替换. 令 $A$ 表示树形图，那么由凯莱定理(定理 2.1)，有 144

$$A(x)=\sum_{n=1}^{\infty}n^{n-1}\frac{x^n}{n!}. \tag{14.17}$$

(这里比凯莱定理中的 $n^{n-2}$ 多了一个因子 $n$，这个 $n$ 是由于树形图的根有 $n$ 种选择而产生的.)因为一个 $n$-集到自身的映射有 $n^n$ 个，那么定理 14.2 的方法表明下述关系成立：

$$\Pi(A(x))=\frac{1}{1-A(x)}=\sum_{n=0}^{\infty}n^n\frac{x^n}{n!}. \tag{14.18}$$

此后我们将证明这个式子.

下述复分析里的著名结果，称为*拉格朗日反演公式*，在与生成函数有关的一些组合问题中起着重要作用. 在许多有关分析的教科书中可以见到这个反演公式的解析证明，见评注. 也可以在形式幂级数理论范围内(利用形式导数等)证明这个定理. 在附录 2 里，我们给出这样一个证明.

**定理 14.3** *设 $f$ 在 $z=0$ 的一个邻域里是解析的且 $f(0)\neq 0$. 那么若 $w=z/f(z)$，$z$ 可以表示为具有正收敛半径的幂级数 $z=\sum_{k=1}^{\infty}c_kw^k$，其中*

$$c_k=\frac{1}{k!}\left\{\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^{k-1}(f(z))^k\right\}_{z=0}. \tag{14.19}$$

**例 14.14** 我们将给出定理 2.1 的第四个证明. 令 $T$ 是"标号树"结构. 我们要证明 $t_n=n^{n-2}$，其中 $n\geqslant 1$. 如果 $A$ 表示前述的树形图，那么显然有 $a_n=nt_n$，即 $A(x)=xT'(x)$. 此外，由定理 14.2 可看出，$\exp(A(x))$是"有根森林"($=F$)结构的指数生成函数. 把 $n+1$ 个顶点上的标号树视为以顶点 $n+1$ 为根的树形图，然后去掉根及其关联的边. 这样就得到一个 $n$ 个顶点的有根森林. 因为这个过程是可逆的，所以我们就建立了一一对应关系. 因此有 145

$$\mathrm{e}^{A(x)}=1+\sum_{n=1}^{\infty}f_n\frac{x^n}{n!}=\sum_{n=0}^{\infty}t_{n+1}\frac{x^n}{n!}=T'(x)=x^{-1}A(x), \tag{14.20}$$

即

$$\frac{A(x)}{\mathrm{e}^{A(x)}}=x. \tag{14.21}$$

取 $z=A(x)$，$f(z)=\mathrm{e}^z=\mathrm{e}^{A(x)}$，$w=x$，把定理 14.3 用到式(14.21)，我们得到 $A(x)=\sum_{k=1}^{\infty}c_kx^k$，其中

$$c_k=\frac{1}{k!}\left\{\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^{k-1}\mathrm{e}^{kz}\right\}_{z=0}=\frac{k^{k-1}}{k!},$$

由此得到 $t_n=n^{n-2}$. 进而，我们看出 $n$ 个顶点的标号有根森林的数目为$(n+1)^{n-1}$.

**注记** 因由(14.20)可得 $A'(x)=\mathrm{e}^{A(x)}+x\mathrm{e}^{A(x)}A'(x)$，即

$$\sum_{n=1}^{\infty} n^n \frac{x^n}{n!} = xA'(x) = \frac{x\mathrm{e}^{A(x)}}{1 - x\mathrm{e}^{A(x)}} = \frac{A(x)}{1 - A(x)},$$

因此就证明了(14.18).

**注记** 在例 14.14 中我们用过的从 $n+1$ 个点的组合结构里去掉一个点的方法，称为导数，的确它对应于生成函数的导数. 另一个例子是从 $n+1$ 个顶点的定向圈上去掉一个顶点，这样就产生一条 $n$ 个顶点的定向路，$n$ 个顶点的定向路有 $n!$ 条. 同样，它们的指数生成函数是 $(1-x)^{-1}$，即 $C'(x)$.

**问题 14E** 令 $a_n$ 表示一个凸 $n+1$ 边形用它的互不相交的弦将其分为四边形的方式数，按常规，取 $a_0=0$，$a_1=1$. 证明对 $n\geqslant 3$ 有递推关系 $\sum_{k+l+m=n} a_k a_l a_m = a_n$. 如果 $f(x)$ 是序列 $a_n$ 的普通生成函数，求 $f(x)$ 的函数方程，并应用定理 14.3 求解这个方程(注意，所得到的结果也可以组合地证明).

146

虽然我们强调，在多数情况下，把幂级数视为形式幂级数，但在若干例子里，显然分析工具在许多组合问题里起着重要作用. 我们再举一例子，说明在许多递推关系中可使用的一个方法.

**例 14.15** 在例 14.11 中，我们遇到递推关系

$$a_n = a_{n-1} + (n-1)a_{n-2} \tag{14.22}$$

和相应的指数生成函数. 在前述例子里，我们已表明了计数函数或大或小地与 $c^n$ 的增长类似，其中 $c$ 为某个常数. 显然 $a_n$ 增长更快，但它的渐近行为的一个好的逼近是什么呢? 得到这个问题答案的第一步涉及一个方法，这个方法可以用到许多递推关系上. 在(14.22)里，我们取

$$a_n = \int_C \psi(z) z^n \mathrm{d}z, \tag{14.23}$$

其中 $C$ 为在 $\mathbb{C}$ 中可以选取的积分路径，$\psi$ 是一个函数，$\psi$ 也可进一步确定. 把(14.23)代入(14.22). 项 $(n-1)a_{n-2}$ 就变为 $\int_C \psi(z)(n-1)z^{n-2}\mathrm{d}z$，分部积分后，我们可以适当地选取 $C$，使这个积分只与 $\psi'(z)$ 有关，而其他项为 0. 这样(14.22)式就变为

$$\int_C \{\psi(z)[z^n - z^{n-1}] + \psi'(z)z^{n-1}\}\mathrm{d}z = 0, \tag{14.24}$$

如果 $\psi(z)(1-z)=\psi'(z)$，即 $\psi(z)=\alpha \mathrm{e}^{z-\frac{1}{2}z^2}$，则对一切 $n\in\mathbb{N}$ 式(14.24)成立. 一旦函数 $\psi$ 已知，那么对 $C$ 的要求表明，从 $-\infty$ 到 $\infty$ 的整个实轴就是积分路径的一个好的选取. 由 $a_0=1$，可推出 $\alpha=(2\pi\mathrm{e})^{-\frac{1}{2}}$.

为了找出 $a_n$ 的渐近行为，我们必须分析函数

147

$$I := \int_{-\infty}^{\infty} \mathrm{e}^{x-\frac{1}{2}x^2} x^n \mathrm{d}x \tag{14.25}$$

的行为. 因为被积函数在 $x=\sqrt{n}$ 附近达到最大，所以将 $x=y+\sqrt{n}$ 代入，则得

$$I = \mathrm{e}^{-\frac{1}{2}n+\sqrt{n}} n^{\frac{1}{2}n} \int_{-\infty}^{\infty} \mathrm{e}^{y-\frac{1}{2}y^2} \exp\left(-y\sqrt{n} + n\log\left(1+\frac{y}{\sqrt{n}}\right)\right)\mathrm{d}y. \tag{14.26}$$

注意，如果 $u$ 和 $v$ 是负的，那么 $|\mathrm{e}^u-\mathrm{e}^v|<|u-v|$，再应用表示式 $\log(1+t)=\int_0^t \frac{\mathrm{d}s}{1+s}=s-\frac{s^2}{2}+\int_0^t \frac{s^2}{1+s}\mathrm{d}s$ 得到

$$\left|-y\sqrt{n}+n\log\left(1+\frac{y}{\sqrt{n}}\right)+\frac{y^2}{2}\right|\leqslant\frac{|y|^3}{\sqrt{n}}.$$

将其代入(14.26)，证明积分趋近于

$$\int_{-\infty}^{\infty}\mathrm{e}^{y-y^2}\mathrm{d}y=\sqrt{\pi}\mathrm{e}^{\frac{1}{4}}.$$

这样我们就证明了

$$a_n\sim\frac{\mathrm{e}^{-\frac{1}{4}}}{\sqrt{2}}n^{\frac{1}{2}n}\mathrm{e}^{-\frac{1}{2}n+\sqrt{n}}. \tag{14.27}$$

显然，不可能用更容易的方法来得到这个结果.

**问题 14F** 令 $F_n(x)$ 表示 $(1-x^n)^{-\mu(n)/n}$ 展开的幂级数. 证明 $\mathrm{e}^x$ 的形式幂级数与 $F_n(x)$ 之间的关系为

$$\mathrm{e}^x=\prod_{n=1}^{\infty}F_n(x).$$

**问题 14G** 求出 $n\times n$ 置换矩阵个数的指数生成函数.

**问题 14H** 将 $n$ 个 0 和 $n$ 个 1 按任意顺序排成一个圆圈，证明一定能给圆圈上这 $2n$ 个位置相继编号为 1，2，…，$2n$，使得这个(0，1)-序列满足(14.13)，但式中的严格不等号“$<$”要改为“$\leqslant$”.

148

**问题 14I** 一个圆周上有 $2n$ 个点，它们的(相继)编号为 1，2，…，$2n$，将这 $2n$ 个点用不相交的 $n$ 条弦一对一对连起来，问有多少种不同的连法？

**问题 14J** 求出 $n$ 个顶点的 2 正则标号图的数目的指数生成函数.

**问题 14K** 讨论 $X$-$Y$ 平面上的步路，其中每一步是 $R:(x,y)\to(x+1,y)$ 或 $U:(x,y)\to(x,y+1)$. 问从(0，0)出发不允许通过点 $(2i-1,2i-1)$，$1\leqslant i\leqslant n$，而到达点 $(2n,2n)$ 有多少种不同的步路？证明这个数是卡塔兰数 $u_{2n+1}$.

**问题 14L** 考虑 $X$-$Y$ 平面上的步路，其中每一步是 $R:(x,y)\to(x+1,y)$ 或 $U_a:(x,y)\to(x,y+a)$，其中 $a$ 为正整数. 有 5 条步路包含直线 $x+y=2$ 上的一个点，即 $RR$，$RU_1$，$U_1R$，$U_1U_1$ 和 $U_2$. 令 $a_n$ 表示包含直线 $x+y=n$ 上一个点的步路的数目(因此 $a_2=5$). 证明 $a_n=F_{2n}$，其中 $F_n$ 是斐波那契数并且 $F_0=F_1=1$.

**问题 14M** 计算函数对 $(f,g)$ 的数目，其中 $f$ 是 $\{1,2,\cdots,r\}$ 到 $\{1,2,\cdots,n\}$ 的映射，$g$ 是使 $f$ 逐点像不变的 $\{1,2,\cdots,n\}$ 上的置换. 对 $n\geqslant r$，用两种解释方式证明

$$\sum_{k=1}^{n}\binom{n}{k}k^r d_{n-k}=B(r)\cdot n!,$$

其中 $d_m$ 表示 1，2，…，$m$ 的更列排列数且 $B(r)$ 是贝尔数.

**问题 14N** 考虑 $X$-$Y$ 平面上的步路，其中每一步是 $R:(x,y)\to(x+1,y)$，$U:(x,y)\to$

$(x, y+1)$或者 $D:(x, y)\to(x+1, y+1)$. 计算从$(0, 0)$到$(n, n)$且不超过直线 $x=y$ 的步路的条数. 求出像(14.10)式那样的步路数的递推关系.

149

## 评注

本章内容的更广泛的讨论，参见 Goulden and Jackson(1983)及 Stanley(1986). 一个可读性很强的综述见 Stanley(1978).

上面提到的第一个参考文献里，关于形式幂级数理论的讨论很多. 关于幂级数理论这一专题也请参见 Niven(1969)以及附录 2. 一般来说，幂级数运算是形式的，并且当由有限次运算确定和式或积式中项 $x^n$ 的系数时，不需讨论收敛性(即极限). 例如，$\sum_{n=0}^{\infty}\left(\frac{1}{2}+x\right)^n$ 在形式运算中是不允许的，因为即使是常数项也不是有限和；但 $\sum_{n=0}^{\infty}(n!\ x+x^2)^n$ 是允许的(即使对 $x\neq 0$ 它不收敛)，因为 $x$ 的任意幂的系数只需有限次计算(参见问题 14F).

人们通常学习解的第一个线性递推关系是 $a_{n+1}=a_n+a_{n-1}$. 它的解就是著名的斐波那契(Fibonacci)序列，参见问题 14A. 在第 10 章中我们已看到，这个名字归功于 Lucas，这个序列与 Leonardo of Pisa(裴波那契的原名)的著作《Liber abaci》(1203)中的一个问题有关.

在例 14.5 中，$n$ 个方格的多方块牌的个数 $a_n<c^n$(其中我们取 $c=15$). 注意这个结论由 Fekete 引理也可推出. 我们是通过对小方格进行适当的编码导出不等式的. 读者可以尝试应用(14.3)式和归纳法，对适当的 $c$ 值证明 $a(m, n)<m\cdot c^n$. (14.9)后面的注记是基于 Stanley(1986)中的结论得到的，这个结论是 D. Hickerson 的一个未发表的组合证明.

例 14.6 的结果与$\mathbb{F}_{p^n}$有一个子域$\mathbb{F}_{p^d}$这一事实有关，其中 $d$ 整除 $n$. 由此人们得到 $x^{p^n}-x$ 是具有 $d$ 整除 $n$ 的域$\mathbb{F}_p$ 上所有不可约多项式之积. 这样就得到了这个例子中已证明的公式.

尽管解为卡塔兰数的问题有广泛的文献，但这些问题还是经常地反复出现(如杂志中的问题部分). 前面已提过，比利时数学家卡塔兰(E. Catalan，1814—1894)研究过加括号的例子(例 14.7).

150

法国组合数学家 D. André(1840—1917)把图 14.2 的反射原理应用于求解贝特朗(Bertrand)的著名的投票问题：在一次选举结束时，如果候选人 $P$ 得到 $p$ 张票，候选人 $Q$ 得到 $q$ 张票，并且 $p<q$，那么在选举过程中，候选人 $Q$ 总是领先的概率为$(q-p)/(q+p)$.

拉格朗日反演公式是拉格朗日对数学分析所做的许多贡献之一(见第 19 章的评注). 它的证明见 Whittaker and Watson(1927)中 7.32 节，这个定理发表于 1770 年. 读者也可参见 G. N. Raney(1960).

## 参考文献


E. Catalan (1838), Note sur une équation aux différences finies, *J. M. Pures Appl.* **3**, 508–516.

I. P. Goulden and D. M. Jackson (1983), *Combinatorial Enumeration*, Wiley-Interscience.

A. Joyal (1981), Une théorie combinatoire des séries formelles, *Advances in Mathematics* **42**, 1–82.

D. A. Klarner (1967), Cell growth problem, *Canad. J. Math.* **19**, 851–863.

I. Niven (1969), Formal power series, *Amer. Math. Monthly* **76**, 871–889.

G. N. Raney (1960), Functional composition patterns and power series reversion, *Trans. Amer. Math. Soc.* **94**, 441–451.

R. P. Stanley (1978), Generating functions, pp. 100–141 in *Studies in Combinatorics* (G.-C. Rota, ed.), Studies in Math. **17**, Math. Assoc. of America.

R. P. Stanley (1986), *Enumerative Combinatorics*, Vol. I, Wadsworth and Brooks/Cole.

E. T. Whittaker and G. N. Watson (1927), *A Course in Modern Analysis*, Cambridge University Press.

151

# 第15章 分　　拆

在前几章中我们已经讨论过一些分拆问题. 现在我们处理最困难的一个分拆问题，即 $n$ 分成 $k$ 部分的无序分拆. 定义 $p_k(n)$ 为

$$n = x_1 + x_2 + \cdots + x_k, \quad x_1 \geqslant x_2 \geqslant \cdots \geqslant x_k \geqslant 1 \tag{15.1}$$

的解的个数. 例如，$7=5+1+1=4+2+1=3+3+1=3+2+2$，于是 $p_3(7)=4$.

利用与定理 13.1 的推论中所用的相同思想，我们看到 $P_k(n)$ 等于 $n-k=y_1+\cdots+y_k(y_1\geqslant\cdots\geqslant y_k\geqslant 0)$ 的解的个数. 如果恰有 $s$ 个整数 $y_i$ 是正的，则由(15.1)有 $p_s(n-k)$ 个解 $(y_1, \cdots, y_k)$. 所以

$$p_k(n) = \sum_{s=1}^{k} p_s(n-k). \tag{15.2}$$

**问题 15A** 证明 $p_k(n)=p_{k-1}(n-1)+p_k(n-k)$ 并用它证明(15.2).

因为对 $n<k$ 有平凡的初始条件 $p_k(n)=0$，又 $p_k(k)=1$，我们可以递归地计算 $p_k(n)$. 显然 $p_1(n)=1$，$p_2(n)=\lfloor n/2 \rfloor$.

**例 15.1** 我们用可以用于其他 $k$ 的方法证明 $p_3(n)=\left\{\frac{n^2}{12}\right\}$，即最接近 $\frac{n^2}{12}$ 的整数. 设 $a_3(n)$ 表示 $n=x_1+x_2+x_3(x_1\geqslant x_2\geqslant x_3\geqslant 0)$ 的解的个数，则 $a_3(n)=p_3(n+3)$. 又设 $y_3=x_3$，$y_2=x_2-x_3$，$y_1=x_1-x_2$，我们看到 $a_3(n)$ 是 $n=y_1+2y_2+3y_3(y_i\geqslant 0, i=1, 2, 3)$ 的解的个数. 所以(参见例 14.2)

152

$$\sum_{n=0}^{\infty} a_3(n)x^n = (1-x)^{-1}(1-x^2)^{-1}(1-x^3)^{-1}. \tag{15.3}$$

设 $\omega=e^{2\pi i/3}$，(15.3)的部分分式分解给出

$$\begin{aligned}\sum_{n=0}^{\infty} a_3(n)x^n =& \frac{1}{6}(1-x)^{-3} + \frac{1}{4}(1-x)^{-2} + \frac{17}{72}(1-x)^{-1} \\ &+ \frac{1}{8}(1+x)^{-1} + \frac{1}{9}(1-\omega x)^{-1} + \frac{1}{9}(1-\omega^2 x)^{-1}.\end{aligned} \tag{15.4}$$

利用(10.6)，从(15.4)我们发现

$$a_3(n) = \frac{1}{12}(n+3)^2 - \frac{7}{72} + \frac{(-1)^n}{8} + \frac{1}{9}(\omega^n + \omega^{2n}),$$

并且这个式子蕴涵着

$$\left| a_3(n) - \frac{1}{12}(n+3)^2 \right| \leqslant \frac{7}{72} + \frac{1}{8} + \frac{2}{9} < \frac{1}{2}.$$

所以

$$p_3(n) = \left\{\frac{1}{12}n^2\right\}. \tag{15.5}$$

**问题 15B** 我们选择正 $n$ 边形的三个顶点并考虑它们构成的三角形. 直接证明按这种方式

可以构成$\left\{\frac{1}{12}n^2\right\}$个互相不叠合的三角形，由此给出(15.5)的第二个证明.

我们将要证明(15.5)是一个更普遍的结果的例子.

**定理 15.1** 如果$k$固定，则

$$p_k(n) \sim \frac{n^{k-1}}{k!(k-1)!} \quad (n \to \infty).$$

[153]

**证明** (i)如果$n=x_1+\cdots+x_k$，$x_1\geqslant\cdots\geqslant x_k\geqslant 1$，则$(x_1, \cdots, x_k)$的排列$k!$产生(13.2)的正整数解，它们不必全不相同. 于是

$$k!p_k(n) \geqslant \binom{n-1}{k-1}. \tag{15.6}$$

如果$n=x_1+\cdots+x_k$，$x_1\geqslant\cdots\geqslant x_k\geqslant 1$，则当$y_i:=x_i+(k-i)(1\leqslant i\leqslant k)$时，整数$y_i$各不相同且$y_1+\cdots+y_k=n+\frac{k(k-1)}{2}$. 所以

$$k!p_k(n) \leqslant \binom{n+\frac{k(k-1)}{2}-1}{k-1}. \tag{15.7}$$

定理的结果由(15.8)和(15.7)得出. ■

**问题 15C** 设$a_1$，$a_2$，…，$a_t$是最大公因子为1的正整数(不必各不相同). 设$f(n)$表示

$$n = a_1x_1 + a_2x_2 + \cdots + a_tx_t$$

的非负整数解$x_1$，…，$x_t$的个数. 生成函数$F(x):=\sum f(n)x^n$是什么? 证明对某个常数$c$，$f(n)\sim cn^{t-1}$，并且作为$a_1$，…，$a_t$的函数明确地给出$c$.

在定理13.1的推论中我们所考虑的问题涉及所谓的$n$分成$k$部分合成的数目. 由这个推论，$n$的合成的总数等于$\sum_{k=1}^{n}\binom{n-1}{k-1}=2^{n-1}$. 在定理13.1中我们所用的方法对此直接证明如下：考虑$n$个蓝色的球，任意两个球之间如果我们愿意的话可以放一个红色的球. 依这种方式形成的构形总数显然是$2^{n-1}$，且它们表示了$n$的所有合成. 不利用第13章的知识，我们可如下证明同一结果：设$c_{nk}$表示$n$分成$k$部分合成的数目. 定义

$$c_k(x) := \sum_{n=k}^{\infty} c_{nk}x^n.$$

[154]

然后，利用前面我们已经用过几次的方法，得到

$$c_k(x) = (x + x^2 + x^3 + \cdots)^k = x^k(1-x)^{-k} = \sum_{n=k}^{\infty}\binom{n-1}{k-1}x^n,$$

而且

$$\sum_{k=1}^{\infty} c_k(x) = \sum_{k=1}^{\infty} x^k(1-x)^{-k} = \frac{x}{1-2x},$$

即$n$有$2^{n-1}$种合成.

**问题 15D** 证明$n\geqslant 4$时，$n$的所有$2^{n-1}$种合成中，整数3恰出现$n\cdot 2^{n-5}$次.

在组合学的这一领域中，最困难且在数学上最为有趣和重要的函数由

$$p(n):=n\text{ 的无序分拆数} \tag{15.8}$$

定义．例如，$p(5)=7$，5 的分拆是

$$1+1+1+1+1=2+1+1+1=3+1+1=2+2+1=4+1=3+2=5.$$

显然，$p(n)$是

$$n=x_1+x_2+\cdots+x_n \quad (x_1\geqslant x_2\geqslant\cdots\geqslant x_n\geqslant 0) \tag{15.9}$$

的解的数目．正如我们在上面看到的，这也可以作为 $n=y_1+2y_2+\cdots+ny_n$ 的解的数目，其中 $y_i\geqslant 0$，$1\leqslant i\leqslant n$.（式中 $y_i$ 表示在第一个定义中等于 $i$ 的项 $x_k$ 的数目.）

所谓的分拆函数 $p(n)$的研究已产生了解析数论、分析、代数几何等一些最引人入胜的领域．显而易见的是，我们仅能考察由组合论据证明的性质.

**定理 15.2** *分拆函数的生成函数是*

155

$$P(x):=\sum_{n=0}^{\infty}p(n)x^n=\prod_{k=1}^{\infty}(1-x^k)^{-1}.$$

**证明** 我们再次使用例 14.2 中的思想．$r_i$ 项等于 $i(1\leqslant i\leqslant m)$的 $n=\sum_{i=1}^{m}ir_i$ 的分拆对应(形式上的)无穷乘积 $\Pi(1+x_k+x_k^2+\cdots)$中的项 $x_1^{r_1}\cdots x_m^{r_m}$．用 $x^k$ 代替 $x_k$，我们得到这个结论． ■

关于分拆的许多定理可以很容易地由点图表示每个分拆来证明，这种图称为 Ferrers 图．在这里分拆中的每一项我们用一行点表示，项以递减的次序，表示最大项的一行点在最上面．有时用正方形代替圆点更为方便(这种情形的图，有些作者称为杨氏图，但是我们仍称为 Ferrers 图)．例如，图 15.1 中的两个图都表示 12 的分拆(5，4，2，1).

在由列代替行阅读 Ferrers 图时，得到的分拆称为原分拆的共轭分拆，于是 $12=5+4+2+1$ 的共轭分拆是 $12=4+3+2+2+1$．共轭关系是对称的．我们首先用几个简单的例子表明 Ferrers 图的用处.

图 15.1

**定理 15.3** *$n$ 的最大的部分为 $k$ 的分拆数是 $p_k(n)$.*

**证明** 其最大的部分是 $k$ 的每个分拆的共轭分拆有 $k$ 个部分(且反之亦然). ■

**问题 15E** 用 Ferrers 图证明 $n+k$ 分成 $k$ 部分的分拆数等于 $n$ 分成至多 $k$ 部分的分拆数．(这是(15.2).)

在有些情形利用生成函数比用 Ferrers 图更灵活．尽管下一个定理可以用类似于 Ferrers 图的一幅图来证明，但我们用生成函数来证明它.

156

**定理 15.4** *$n$ 分成奇数个部分的分拆数等于 $n$ 分成不相等的部分的分拆数.*

**证明** $n$ 分成奇数个部分的分拆数的生成函数(由定理 15.2 的一个显而易见的推广）是 $\prod_{m=1}^{\infty}(1-x^{2m-1})^{-1}$，而 $n$ 分成不相等的部分的分拆数(由与在定理 15.2 的证明中所用的相同论证)是 $\prod_{k=1}^{\infty}(1+x^k)$．因为

$$\prod_{k=1}^{\infty}(1+x^k)=\prod_{k=1}^{\infty}\frac{(1-x^{2k})}{(1-x^k)}$$
$$=\prod_{k=1}^{\infty}(1-x^{2k})\prod_{l=1}^{\infty}(1-x^l)^{-1}=\prod_{m=1}^{\infty}(1-x^{2m-1})^{-1},$$

证明完成. ■

现在考虑函数$(P(x))^{-1}=\prod_{k=1}^{\infty}(1-x^k)$. 在这个乘积的展开中，$n$ 分成不相等部分的一个分拆，如果部分的数目是偶数，它给 $x^n$ 的系数提供$+1$；如果部分的数目是奇数，它给 $x^n$ 的系数提供$-1$. 于是 $x^n$ 的系数是 $p_e(n)-p_o(n)$，这里 $p_e(n)$和 $p_o(n)$分别表示 $n$ 分成不相等的部分的数目是偶数和奇数时 $n$ 的分拆数. 欧拉曾证明，除了 $n$ 具有形式 $n=\omega(m):=(3m^2-m)/2$ 或 $n=\omega(-m)=(3m^2+m)/2$ 时，$p_e(n)-p_o(n)=(-1)^m$；对其余的 $n$，$p_e(n)=p_o(n)$. 数 $\omega(m)$和 $\omega(-m)$称为五边形数. 关系 $\omega(m)=\sum_{k=0}^{m-1}(3k+1)$和图 15.2 解释了这个名字.

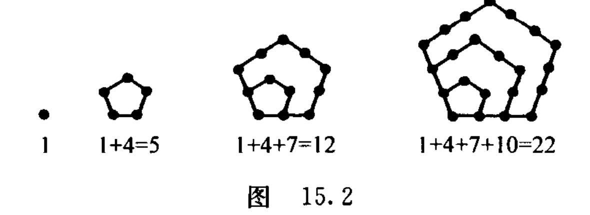



图 15.2

欧拉恒等式的如下极为巧妙的图示证明属于 Franklin(1881).

**定理 15.5**　我们有

$$\prod_{k=1}^{\infty}(1-x^k)=1+\sum_{m=1}^{\infty}(-1)^m(x^{\omega(m)}+x^{\omega(-m)}).$$

**证明**　考虑 $n$ 分成不相等部分的 Ferrers 图，如图 15.3 中的 $23=7+6+5+3+2$.

图中最后一行称为图的底，底上的圆点数用 $b$ 表示. 在图 15.3 中底由 $b=2$ 个圆点的线段表示. 连结最上面一行的最后一个点和这个图形中的其他点的 45°的最长线段称为该图的斜线. 斜线上的点数用 $s$ 表示. 在图 15.3 中，斜线由 $s=3$ 的一条线段表示. 现在我们定义图上的两种运算，它们称为 $A$ 和 $B$.

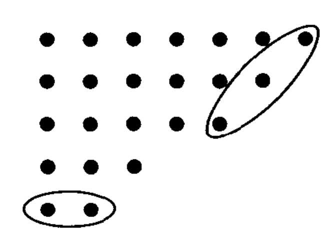


图 15.3

$A$：如果 $b\leqslant s$，则移去底并放在图形的右边形成平行于原来的斜线的新斜线，除非 $b=s$ 且底和斜线有一个公共的点. 这一例外在下面考虑.

$B$：如果 $b>s$，则移去斜线并邻接在图形的底部作为一个新底，除非 $b=s+1$ 且底和斜线有一个公共点.

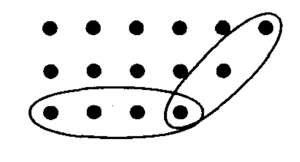


图 15.4

在图 15.3 中，运算 $A$ 可以执行，它产生分拆 $23=8+7+5+3$. 对运算 $B$，例外情况的一个例子如图 15.4 所示.

157

运算 $A$ 的例外仅当

158

$$n=b+(b+1)+\cdots+(2b-1)$$

时发生，即 $n=\omega(b)$. 运算 $B$ 的例外仅当 $n=(s+1)+\cdots+2s$，即 $n=\omega(-s)$ 时发生. 在所有其他情形运算都可以执行，于是我们有 $n$ 分成不相等部分的数目为偶数的分拆和 $n$ 分成不相等部分的数目为奇数的分拆之间的一个一一对应，因此，对 $n$ 的这些值，我们有 $p_e(n)-p_o(n)=0$. 在例外情形，这个差是 1 或者 $-1$. ■

欧拉利用定理 15.5 发现 $p(n)$ 的递推公式如下.

**定理 15.6** 对 $n<0$，设 $p(n)=0$，则对 $n\geqslant 1$，

$$p(n)=\sum_{m=1}^{\infty}(-1)^{m+1}\{p(n-\omega(m))+p(n-\omega(-m))\}. \tag{15.10}$$

**证明** 这是定理 15.2 和定理 15.5 的一个直接推论. ■

注意在(15.10)中和是有限的. 借助这个递推式，对小的 $n$ 值，可以很快地产生 $p(n)$ 的一张表.

这个递推式的前两项与著名的斐波那契递推式相同(参见问题 5E). 尽管接着是两个负项，可以设想 $p(n)$ 的增长方式类似于斐波那契数，即对某个常数 $c$，如同 $c^n$，但情况并非如此. 我们将证明 $p(n)$ 的增长要慢得多，$p(n)$ 的精确逼近涉及解析数论中的复杂方法，我们仅提一下渐近公式的主项：

$$\lim_{n\to\infty}n^{-\frac{1}{2}}\log p(n)=\pi\sqrt{\frac{2}{3}}.$$

159

事实上，可以证明 $p(n)$ 比 $\exp\left(\pi\sqrt{\frac{2}{3}n}\right)$ 要小得多.

**定理 15.7** 对 $n>2$，我们有

$$p(n)<\frac{\pi}{\sqrt{6(n-1)}}e^{\pi\sqrt{\frac{2}{3}n}}.$$

**证明** 设 $f(t):=\log P(t)$，从定理 15.2 我们发现

$$f(t)=-\sum_{k=1}^{\infty}\log(1-t^k)=\sum_{k=1}^{\infty}\sum_{j=1}^{\infty}\frac{t^{kj}}{j}=\sum_{j=1}^{\infty}\frac{j^{-1}t^j}{1-t^j}.$$

从现在起，设 $0<t<1$，则由

$$(1-t)^{-1}(1-t^j)=1+t+\cdots+t^{j-1}>jt^{j-1},$$

我们发现

$$f(t)<\frac{t}{1-t}\sum_{j=1}^{\infty}j^{-2}=\frac{1}{6}\pi^2\frac{t}{1-t}.$$

因为 $p(n)$ 是递增的，我们有 $P(t)>p(n)t^n(1-t)^{-1}$. 通过这两个不等式的结合，然后代入 $t=(1+u)^{-1}$，我们得到

$$\log p(n)<f(t)-n\log t+\log(1-t)$$

$$< \frac{\pi^2}{6} \cdot \frac{t}{1-t} - n \log t + \log(1-t)$$

$$= \frac{\pi^2}{6} u^{-1} + n \log(1+u) + \log \frac{u}{1+u}.$$

因此

$$\log p(n) < \frac{1}{6}\pi^2 u^{-1} + (n-1)u + \log u.$$

代入 $u=\pi\{6(n-1)\}^{-\frac{1}{2}}$，我们获得所要的不等式. ■

欧拉恒等式是著名的雅可比恒等式的特例，后者在 $\theta$ 函数论中很重要. 如果我们不知道利用 Ferrers 图对所谓雅可比三重积恒等式的优美的组合证明，就不会提到这个式子，这个证明属于 Wright(1965). 160

**定理 15.8** 我们有

$$\prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}t)(1+q^{2n-1}t^{-1}) = \sum_{r=-\infty}^{\infty} q^{r^2} t^r.$$

**证明** 我们把这一断言改写成

$$\prod_{n=1}^{\infty}(1+q^{2n-1}t)(1+q^{2n-1}t^{-1}) = \sum_{r=-\infty}^{\infty} q^{r^2} t^r \prod_{n=1}^{\infty}(1-q^{2n})^{-1},$$

并代入 $x=qt$，$y=qt^{-1}$. 这产生关系

$$\prod_{n=1}^{\infty}\{(1+x^n y^{n-1})(1+x^{n-1}y^n)\}$$
$$= \sum_{r=-\infty}^{\infty} x^{\frac{1}{2}r(r+1)} y^{\frac{1}{2}r(r-1)} \prod_{n=1}^{\infty}(1-x^n y^n)^{-1}. \tag{15.11}$$

我们通过把等式两边解释成与适当的组合对象的计数对应的生成函数，然后证明这些对象之间的一个一一对应来证明这个关系. 对等式的左边，我们找到高斯整数 $n+mi$ 分成 $a+(a-1)i$ 和 $(b-1)+bi(a\geqslant 1,b\geqslant 1)$ 且没有两部分相等的分拆数的生成函数作为一个组合学解释，称这个数为 $\alpha(n,m)$. 于是(15.11) 的左边是 $\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\alpha(n,m)x^n y^m$. 对等式的右边，利用定理 15.2 并用 $\sum_{k=1}^{\infty}p(k)x^k y^k$ 代替那个乘积. 因此，我们必须证明 $\alpha(n,m)=p(k)$，其中 $n=k+\frac{1}{2}r(r+1)$ 且 $m=k+\frac{1}{2}r(r-1)$. 不失一般性，我们假设 $n\geqslant m$，即 $r\geqslant 0$. $n+mi$ 的一个分拆一定有 $v\geqslant 0$ 个类型为 $(b-1)+bi$ 的项和 $v+r$ 个类型为 $a+(a-1)i$ 的项，且 $n\geqslant \frac{1}{2}r(r+1)$，因此 $k\geqslant 0$. 在图 15.5 中，我们考虑 $(n,m)=(47,44)$，于是 $r=3$ 且 $k=41$. 取 $41=12+10+8+5+2+2+$

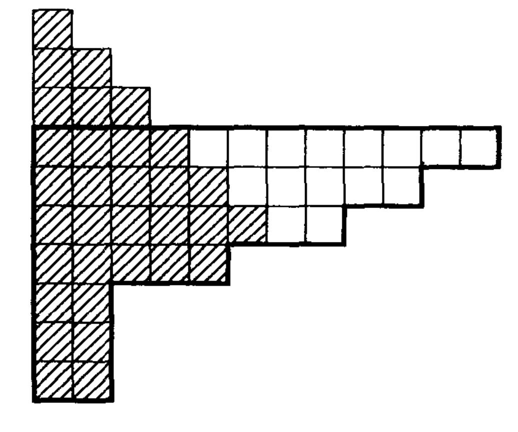


图　15.5

2 的 Ferrers 图并在最上面一行的上方加上长度为 $r, r-1, \cdots, 1$ 的行.

得到的图被分成两部分，左边的阴影部分由从在上面加上的部分开始的“楼梯”确定. 我们按列阅读阴影部分. 按这一方法，序列是递减的，这些数是类型为 $a+(a-1)i$ 的项中的 $a$. 按行阅读不是阴影的部分，序列也是递减的，这些数是类型为 $(b-1)+bi$ 的项中的 $b-1$（最后的 $b$ 可以是 1，对应于一个不是阴影的空行）. $a$ 的数目比 $b-1$ 的数目多 $r$，$a$ 的和显然比 $b-1$ 的和多 $k+\frac{1}{2}r(r+1)$. 于是，我们确实已经产生了所需类型的 $n+mi$ 的一个分拆. 容易看到这个过程是可以逆转的，即我们已经定义了我们所寻找的一一对应. ■

**问题 15F** 证明 $n$ 的自共轭分拆的数目等于 $n$ 分成不相等的奇数部分的分拆数.

关于分拆，我们要考虑的最后一个问题以杨氏表或标准表著称. 形状为 $(n_1, n_2, \cdots, n_m)$ 的杨氏表是一幅正方形的 Ferrers 图（或杨氏图），整数 1 到 $n$ 写在正方形中（一个正方形中一个数字），使得所有的行和所有的列是递增的. 例如，图 15.6 显示了一张形状为 (5, 4, 2, 1) 的杨氏表.

161 ~ 162

我们对确定形状给定的杨氏表的数目感兴趣. 首先，这显得有些不自然，然而，杨氏表在群表示论（以及其他领域）有重要作用. 关于这些表的一个有趣事实是，有 $n$ 个正方形（称为“腔”）的杨氏表和 1 到 $n$ 的对合之间存在一个一一对应.（注意我们因此可以用问题 14G 对杨氏表的整个数目进行计数.）对这个一一对应以及几个相关问题的处理我们参考 D. Knuth(1973).

| 1 | 3 | 4 | 7 | 11 |
|---|---|---|---|---|
| 2 | 5 | 10 | 12 | |
| 6 | 9 | | | |
| 8 | | | | |

图 15.6

为了对给定形状的杨氏表进行计数，我们需引入由

$$\Delta(x_1, \cdots, x_m) := \prod_{1\leqslant i<j\leqslant m}(x_i - x_j) \tag{15.12}$$

定义的函数 $\Delta(x_1, \cdots, x_m)$.（注意，$\Delta$ 是范德蒙德行列式的值.）

**引理 15.9** 设

$$\begin{aligned} g(x_1, \cdots, x_m; y) := & x_1\Delta(x_1+y, x_2, \cdots, x_m) \\ & + x_2\Delta(x_1, x_2+y, \cdots, x_m) + \cdots + x_m\Delta(x_1, x_2, \cdots, x_m+y), \end{aligned}$$

则

$$g(x_1, \cdots, x_m; y) = \left(x_1 + \cdots + x_m + \binom{m}{2}y\right)\Delta(x_1, \cdots, x_m).$$

**证明** 显然，函数 $g$ 是次数为 $1+\deg\Delta(x_1, \cdots, x_m)$ 的齐次多项式，其变量为 $x_1, \cdots, x_m, y$. 如果我们互换 $x_i$ 和 $x_j$，则 $g$ 变号. 于是，如果 $x_i=x_j$，则 $g$ 一定为 0，即 $g$ 能被 $x_i-x_j$ 整除，因此能被 $\Delta(x_1, \cdots, x_m)$ 整除. 如果 $y=0$，断言是明显的. 所以，我们只需证明 $y$ 的系数为 $\binom{m}{2}$. 如果我们展开 $g$，$y$ 的一次项是 $\frac{x_i y}{x_i-x_j}\Delta(x_1, \cdots, x_m)$ 和 $\frac{-x_j y}{x_i-x_j}\Delta(x_1, \cdots, x_m)$，这些项取自 $1\leqslant i<j\leqslant m$ 的所有数对 $(i, j)$. 这些项的和显然是 $\binom{m}{2}\Delta(x_1, \cdots, x_m)$. ■

163

我们引入定义在所有 $m$ 元组 $(n_1, \cdots, n_m)$ 上的一个函数 $f$，$m\geqslant 1$，它有如下性质：

$$f(n_1,\cdots,n_m)=0\quad 除非\ n_1\geqslant n_2\geqslant\cdots\geqslant 0;\tag{15.13}$$

$$f(n_1,\cdots,n_m,0)=f(n_1,\cdots,n_m);\tag{15.14}$$

$$f(n_1,\cdots,n_m)=f(n_1-1,n_2,\cdots,n_m)+f(n_1,n_2-1,\cdots,n_m)+\cdots+f(n_1,n_2,\cdots,n_m-1),$$
$$如果\ n_1\geqslant n_2\geqslant\cdots\geqslant n_m\geqslant 0;\tag{15.15}$$

$$f(n)=1\quad 如果\ n\geqslant 0.\tag{15.16}$$

显然 $f$ 被很好地定义了. 我们断言 $f(n_1,\ \cdots,\ n_m)$给出了形状为$(n_1,\ \cdots,\ n_m)$的杨氏表的计数. 条件(15.13)是显然的，而且(15.14)和(15.16)也是如此. 为了看出形状为$(n_1,\ \cdots,\ n_m)$的杨氏表的数目满足(15.15)，我们考虑项 $n$，它必定是在一行的最后一项，而且如果我们移去有 $n$ 的正方形，那么就得到 $n-1$ 的杨氏表. 事实上，如果表中有两行或更多的行有相同的长度，则 $n$ 只能是它们之中最靠下的一行的最末一项；但对在(15.15)中包含的所有项并不碍事，因为比如说 $n_1=n_2$，则 $f(n_1-1,\ n_2,\ \cdots,\ n_m)=0$.

**定理 15.10**　*具有形状$(n_1,\ \cdots,\ n_m)$的杨氏表的数目满足*

$$f(n_1,\cdots,n_m)=\frac{\Delta(n_1+m-1,n_2+m-2,\cdots,n_m)n!}{(n_1+m-1)!(n_2+m-2)!\cdots n_m!},\tag{15.17}$$

*且事实上，如果 $n_1+m-1\geqslant n_2+m-2\geqslant\cdots\geqslant n_m$，$f$ 的公式是正确的.*

164

**证明**　我们首先观察到，如果对某个 $i$，我们有 $n_i+m-i=n_i+1+m-i-1$，那么(15.17)右边的表达式 $\Delta=0$，与不允许这种形状的构形相应. 我们必须证明(15.17)的右边满足(15.13)到(15.16)，但除(15.15)之外它们都是平凡的，通过在引理 15.9 中代入 $x_i=n_i+m-i$ 和 $y=-1$ 我们找到关系式(15.15). ■

这个定理的一个阐述使它更为有趣. 在一张杨氏表中，我们引入"钩"的概念. 在一张杨氏表中，对应于一个腔的钩是这个腔与在同行上右侧的腔及同列上下方的腔的并. "钩的长度"是在钩上的所有腔的数目. 在图 15.7 中，我们显示了一张杨氏图，图中每个腔中的数字等于它对应的钩的长度. 阴影区域是第 2 行第 3 列的腔对应的钩.

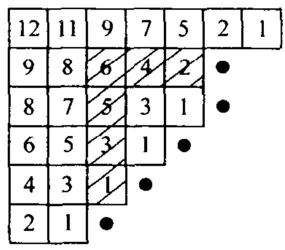


图　15.7

我们现在叙述属于 J. S. Frame，G. de Beanuregard Robinson and R. M. Thrall(1954)的值得注意的定理.

**定理 15.11**　*一个给定形状且总共有 $n$ 个腔的杨氏表的数目等于 $n!$ 除以所有钩的长度之积.*

**证明**　如果我们有一张形状为$(n_1,\ \cdots,\ n_m)$的杨氏表，则对应第 1 行第 1 列的腔的钩的长度为 $n_1+m-1$. 考虑在第 1 行中的腔所对应的钩的长度. 在图 15.7 中，第 2 列的长度与第 1 列的长度相同，因此对应第 2 个腔的钩的长度为 $n_1+m-2$. 对下一个腔，钩的长度减 2，原因是在最后一行由圆点指示的"缺失的腔". 类似地，对有两个点的列，钩的长度减 3. 于是，在第 1 行中钩的长度是从 1 到 $n_1+m-1$ 的数，但$(n_1+m-1)-(n_j+m-j)(2\leqslant j\leqslant m)$的数除外. 类似地，在第 $i$ 行中钩的长度是从 1 到 $n_i+m-i$ 的数，但$(n_i+m-i)-(n_j+m-j)(i+1\leqslant j\leqslant m)$的数除外. 由此，钩的长度之积是$\left\{\prod_{i=1}^{m}(n_i+m-i)!\right\}/\Delta(n_1+m-1,\ \cdots,\ n_m)$. 由引理 15.9，定理得证. ■

165

**问题 15G** 考虑形状为$(n, n)$的一张杨氏表. 定义一个序列 $a_k$，$1\leqslant k\leqslant 2n$，如果 $k$ 在表中的第 $i$ 行，则 $a_k := i$，$i=1$，2. 由此证明这种形状的杨氏表的数目是卡塔兰数 $u_{n+1}$(与定理 15.11 相符).

**问题 15H** 适合大小为 $k\times n-k$ 的盒子的 Ferrers 图有多少?

**问题 15I** 证明：$n$ 分成不能被 $d$ 整除的部分的分拆数等于 $n$ 分成的部分中没有任何部分出现超过 $d-1$ 次的分拆数.

**问题 15J** 定义 $P_n := \prod_{k=1}^{n} k!$. 证明 $P_{n-1}^2 \cdot (n^2)!$ 能被 $P_{2n-1}$整除.

## 评注

利用 Ferrers 图证明像定理 15.3 这样的定理是由 Sylvester 在 1853 年引入的. 他写道，这一证明由 N. M. Ferrers 寄给他.

对涉及 Ferrers 图的其他证明及类似的事项(例如，定理 15.4 的一个证明)参见 Hardy and Wright(1954)、MacMahon(1916)，以及 Van Lint(1974).

定理 15.5 的欧拉证明用的是归纳法，多边形数出现在古代的数学中，例如毕达哥拉斯(Pythagoras)在公元前 500 年之前考虑过三角形数.

定理 15.7 属于 Van Lint(1974).

分拆函数 $p(n)$的渐近行为由 G. H. Hardy and S. Ramanujan(1918)在一篇论文中给出，其中他们发展的著名的"圆法"在数论中有许多应用. 一个进一步的渐近结果由 H. Rademacher(1937)给出，证明著名的戴德金 $\eta$ 函数

166

$$\eta(z) := e^{\frac{\pi i z}{12}} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z}),$$

这是值得注意的函数方程. 证明的一个阐述见 Chandrasekharan(1970).

雅可比(C. G. J. Jacobi，1804—1851)以发展椭圆函数论而著名. 23 岁时他在哥尼斯堡任教授. 两年后他出版了《Fundamenta Nova Theoriae Functionum Ellipticarum》，在该书的 64 节我们可以找到现在所说的三重积恒等式.

首先使用像图 15.6 那样的图表的是弗罗贝尼乌斯! 1 年以后(1901 年)，A. Young 在他的关于置换群的矩阵表示的工作中独立地引入了图表，杨氏表已成为标准术语.

## 参考文献

K. Chandrasekharan (1970), *Arithmetical Functions*, Springer-Verlag.

J. S. Frame, G. de Beauregard Robinson, and R. M. Thrall (1954), The hook graphs of $S_n$, *Canad. J. Math.* **6**, 316–324.

F. Franklin (1881), Sur le développement du produit infini $(1 - x)(1-x^2)(1-x^3)(1-x^4)\cdots$, *Comptes Rendus Acad. Sci.* (Paris) **92**, 448–450.

G. H. Hardy and S. Ramanujan (1918), Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc.* (2) **17**, 75–115.

G. H. Hardy and E. M. Wright (1954), *An Introduction to the Theory of Numbers*, 3d edn., Clarendon Press.

D. Knuth (1973), *The Art of Computer Programming*, Vol. 3, Addison-Wesley .

J. H. van Lint (1974), *Combinatorial Theory Seminar Eindhoven University of Technology*, Lecture Notes in Math. **382**, Springer-Verlag.

P. A. MacMahon (1916), *Combinatory Analysis* Vol. II, Cambridge University Press.

H. Rademacher (1937), On the partition function $p(n)$, *Proc. London Math. Soc.* **43**, 241–254. [167]

E. M. Wright (1965), An enumerative proof of an identity of Jacobi, *J. London Math. Soc.* **40**, 55–57.

A. Young (1901), On quantitative substitutional analysis, *Proc. London Math. Soc.* **33**, 97–146. [168]

# 第16章 (0, 1)-矩阵

在前面几章中(0, 1)-矩阵已经出现过几次；尤其是那些有常数直线和的(0, 1)-矩阵引出了有趣的问题. 在本章中，我们将考虑有给定的直线和的(0, 1)-矩阵的存在性问题，并试着在常数直线和的情形对有多少矩阵进行计数或估计. 对第一个问题，矩阵不必是方阵. 如果矩阵 $A$ 的行和是 $r_1$，$r_2\cdots$，$r_k$，那么我们称向量 $\boldsymbol{r}:=(r_1, r_2\cdots, r_k)$ 为 $A$ 的行和，类似地有矩阵的列和.

我们考虑有给定的行和 $\boldsymbol{r}$ 及列和 $\boldsymbol{s}$ 的(0, 1)-矩阵的存在性. 为了方便，我们假定 $\boldsymbol{r}$ 和 $\boldsymbol{s}$ 的坐标是非增的，这就是，$\boldsymbol{r}$ 和 $\boldsymbol{s}$ 是分拆(为本章的目的计，我们允许在分拆中出现零坐标).

给定同一个整数 $N$ 的两个分拆 $\boldsymbol{r}=(r_1, r_2, \cdots, r_n)$ 和 $\boldsymbol{s}=(s_1, s_2, \cdots, s_m)$，当对所有的 $k$，有

$$r_1+r_2+\cdots+r_k\geqslant s_1+s_2+\cdots+s_k$$

时，我们说 $\boldsymbol{r}$ 强于 $\boldsymbol{s}$，当 $k$ 分别超过 $n$ 或 $m$ 时，$r_k$ 或 $s_k$ 视为 0. 回忆一个分拆 $\boldsymbol{r}$ 的共轭是分拆 $\boldsymbol{r}^*$，这里 $r_i^*$ 是使得 $r_j\geqslant i$ 的 $j$ 的数目.

**问题 16A** 证明如下的断言：$\boldsymbol{r}$ 强于 $\boldsymbol{s}$ 当且仅当后者能由一系列运算从前者得到，运算是"取满足 $a\geqslant b+2$ 的两个部分(坐标)$a$ 和 $b$，然后用 $a-1$ 和 $b+1$ 替换它们". (这就是，$\boldsymbol{s}$ 比 $\boldsymbol{r}$ "更为平均".)例如，(5, 4, 1)强于(3, 3, 3, 1)，用这样的运算的序列后者有几种方式能从前者得到，这包括

169

$$(5,4,1,0)\to(5,3,2,0)\to(5,3,1,1)\to(4,3,2,1)\to(3,3,3,1)$$

以及

$$(5,4,1,0)\to(4,4,1,1)\to(4,3,2,1)\to(3,3,3,1).$$

**定理 16.1** 设 $r_1$，$r_2$，$\cdots$，$r_n$ 和 $s_1$，$s_2$，$\cdots$，$s_m$ 是非负整数的两个非增序列，每个序列的和是公共值 $N$. 存在一个行和为 $\boldsymbol{r}$ 且列和为 $\boldsymbol{s}$ 的 $n\times m$(0, 1)-矩阵，当且仅当 $\boldsymbol{r}^*$ 强于 $\boldsymbol{s}$.

**证明** 为证明必要性，设给定 $k$ 并考虑假设的一个行和为 $\boldsymbol{r}$ 且列和为 $\boldsymbol{s}$ 的(0, 1)-矩阵的前 $k$ 列. 在这些列中 1 的个数是

$$s_1+s_2+\cdots+s_k\leqslant\sum_{i=1}^{n}\min(k,r_i)=\sum_{j=1}^{k}r_j^*.$$

后面的等式从分拆 $\boldsymbol{r}$(见图 16.1)的 Ferrers 图来看是极为明显的，我们看到两个表达式给出了前 $k$ 列中腔的计数.

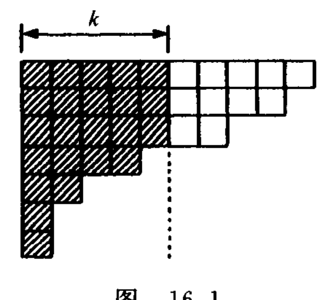



图 16.1

现在我们引入发点为 $S$ 且收点为 $T$ 的一个运输网络，每行用一个 $x_i$ 表示，每列用一个 $y_j$ 表示. 从 $S$ 到 $x_i$ 有一条容量为 $r_i$ 的边，$1\leqslant i\leqslant n$；从 $y_j$ 到 $T$ 有一条容量为 $s_j$ 的边，$1\leqslant j\leqslant m$；且从 $x_i$ 到 $y_j$ 有一条容量为 1 的边，$1\leqslant i\leqslant n$，$1\leqslant j\leqslant m$. 我们断言：存在一个行和为 $\boldsymbol{r}$ 且列和为 $\boldsymbol{s}$ 的(0, 1)-矩阵 $M=(a_{ij})$，当且仅当这个网络容许强度为 $N$ 的一个流(至少有两个容量为 $N$

170

的割，因此它是最大流）．给定这样一个矩阵，通过饱和邻接 $S$ 和 $T$ 的边，并对从 $x_i$ 到 $y_j$ 的边赋以流 $a_{ij}$，我们得到强度为 $N$ 的一个流．反之，如果该网络容许强度为 $N$ 的一个流，则存在同样强度的一个整数流（见定理 7.2）；显然，与 $S$ 或者 $T$ 相邻的边一定是饱和的，在其他边上流必定为 0 或者 1.

考虑在这个网络中分离 $S$ 与 $T$ 的一个割 $A$，$B$．比如说 $A$ 由 $S$、$X:=\{x_i, i=1, \cdots, n\}$ 的 $n_0$ 个顶点，以及 $Y:=\{y_i: i=1, \cdots, m\}$ 的 $m_0$ 个顶点构成．穿过 $A$ 到 $B$ 的边包括离开 $S$ 的 $n-n_0$ 条边、进入 $T$ 的 $m_0$ 条边，以及从 $X$ 到 $Y$ 的 $n_0(m-m_0)$ 条边．这个割的容量至少为

$$r_{n_0+1}+r_{n_0+2}+\cdots+r_n+s_{m-m_0+1}+s_{m-m_0+2}+\cdots+s_m+n_0(m-m_0).$$

参照分拆 $\boldsymbol{r}$ 的 Ferrers 图（见图 16.2）是方便的．在这张 Ferrers 图上，腔的数目是 $N$．于是，很显然 $N$ 至多为 $n_0(m-m_0)$ 加上在最后 $n-n_0$ 行中的腔，再加上在最后 $m_0$ 列中的腔．在最后 $m_0$ 列中的腔的数目是共轭 $\boldsymbol{r}^*$ 的最后 $m_0$ 个部分的和．但在 $\boldsymbol{r}^*$ 强于 $\boldsymbol{s}$ 的假设下，

$$r^*_{m-m_0+1}+r^*_{m-m_0+2}+\cdots+r^*_m\leqslant s_{m-m_0+1}+s_{m-m_0+2}+\cdots+s_m,$$

我们得出结论：任意割的容量至少为 $N$．由最大流-最小割定理，即定理 7.1，所需要的强度为 $N$ 的流存在．■

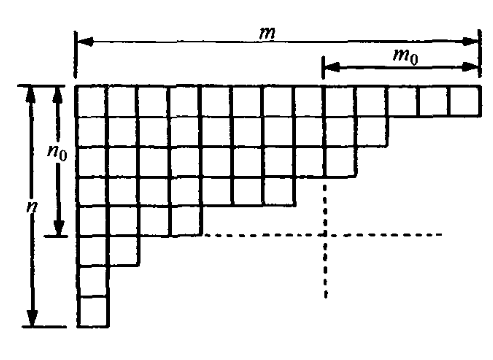


图　16.2

171

为了建立流和（0，1）-矩阵之间的联系，我们给出了上面的证明，但是，可以给出定理 16.1 中条件的充分性的更直接的证明．我们的阐释与由 Krause（1996）给出的相似．

首先假设有一个行和为 $\boldsymbol{r}$ 且列和为 $\boldsymbol{s}_1$ 的（0，1）-矩阵 $A_1$，且从 $\boldsymbol{s}_1$ 由问题 16A 中的运算得到 $\boldsymbol{s}_2$．那么我们断言容易构建一个行和为 $\boldsymbol{r}$ 且列和为 $\boldsymbol{s}_2$ 的（0，1）-矩阵：如果在 $\boldsymbol{s}_1$ 中满足 $a\geqslant b+2$ 的部分 $a$，$b$ 分别是列 $j$ 和列 $k$ 的和，则必有一行 $i$ 使得在 $A_1$ 中 $(i, j)$ 项是 1 且 $(i, k)$ 项是 0；如果交换这两项，就得到想要的矩阵 $A_2$.

现在假定 $\boldsymbol{r}^*$ 强于 $\boldsymbol{s}$．以对应于 $\boldsymbol{r}$ 的 Ferrers 图的矩阵 $A_0$ 开始，为得到大小为 $n\times m$ 的矩阵，在需要时添加全 0 的列．$A_0$ 的列和是 $\boldsymbol{r}^*$，如果 $\boldsymbol{r}^*$ 强于 $\boldsymbol{s}$，我们能找到分拆的一个序列

$$\boldsymbol{r}^*=\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_\ell=\boldsymbol{s}$$

使得这个序列中的每一个分拆由问题 16A 中的运算从前一个分拆得到．由上面的观察，行和为 $\boldsymbol{r}$ 且列和为 $\boldsymbol{s}$ 的（0，1）-矩阵可以从 $A_0$ 经 $\ell$ 次交换的一个序列得到.

**例 16.1**　取 $\boldsymbol{r}=(3, 2, 2, 2, 1)$ 且 $\boldsymbol{s}=(3, 3, 3, 1)$，则 $\boldsymbol{r}^*=(5, 4, 1)$ 强于 $\boldsymbol{s}$．上面描述的算法可能给出如下的矩阵序列：

$$\begin{bmatrix}1&1&1&0\\1&1&0&0\\1&1&0&0\\1&1&0&0\\1&0&0&0\end{bmatrix}\to\begin{bmatrix}1&1&1&0\\0&1&1&0\\1&1&0&0\\1&1&0&0\\1&0&0&0\end{bmatrix}\to\begin{bmatrix}1&1&1&0\\0&1&1&0\\0&1&1&0\\1&1&0&0\\1&0&0&0\end{bmatrix}\to\begin{bmatrix}1&0&1&1\\0&1&1&0\\0&1&1&0\\1&1&0&0\\1&0&0&0\end{bmatrix}$$

172

这里列和向量是

$$(5,4,1,0)\to(4,4,2,0)\to(3,4,3,0)\to(3,3,3,1).$$

(我们并不关心向量不总是非增的情形.)

在下面的定理中，我们扩展这一算法的思想，并找到有特定直线和的(0，1)-矩阵的一个(粗略)估计作为结果.

**定理 16.2** 给定整数 $N$ 的分拆 $\boldsymbol{r}$ 和 $\boldsymbol{s}$，设 $M(\boldsymbol{r},\boldsymbol{s})$ 表示行和为 $\boldsymbol{r}$ 且列和为 $\boldsymbol{s}$ 的(0，1)-矩阵 $A$ 的数目. 如果 $\boldsymbol{r}$ 强于 $\boldsymbol{r}_0$ 且 $\boldsymbol{s}$ 强于 $\boldsymbol{s}_0$，则

$$M(\boldsymbol{r}_0,\boldsymbol{s}_0)\geqslant M(\boldsymbol{r},\boldsymbol{s}).$$

**证明** 我们建立如下的简单观察. 固定长度为 $n$ 的行和向量 $\boldsymbol{r}=(r_1, r_2, \cdots, r_n)$ 以及长度为 $m$ 的列和向量 $\boldsymbol{s}=(s_1, s_2, \cdots, s_m)$，它们有相等的加和(我们不要求它们是非增的). 如果 $s_1>s_2$，那么我们断言

$$M(\boldsymbol{r},(s_1-1,s_2+1,s_3,\cdots,s_m))\geqslant M(\boldsymbol{r},(s_1,s_2,s_3,\cdots,s_m)).$$

当然，不等式对任意两列成立(我们用前两列只是为了记号上的方便). 将同样的思想应用到转置矩阵上，其中保持 $\boldsymbol{s}$ 为常数且把 $r_i$ 和 $r_j$ $(r_i>r_j)$ 换成 $r_i-1$ 和 $r_j+1$，这不会减小与此相联系的(0，1)-矩阵的数目. 从这个观察和问题 16A 的结果得出这一定理的不等式.

为了证明上面的观察，考虑列和为 $(s_3, s_4, \cdots, s_m)$ 的大小为 $n\times(m-2)$ 的(0，1)-矩阵 $A$. 对一个给定的矩阵 $A$，预先计划 $A$ 的两列有时可能有时不可能得出行和 $\boldsymbol{r}$；如果这是可能的，我们需要添加两个 1 到 $a$ 个行、一个 1 到 $b$ 个行，而对 $c$ 个行不添加 1，比如说，其中 $a+b+c=n$，且 $2a+b=s_1+s_2$. 但预先计划两列得到新的列和 $s_1$ 和 $s_2$ 的方法数是

$$\binom{b}{s_1-a}=\binom{b}{s_2-a},$$

而且这至多是预先计划两列得到新的列和 $s_1-1$ 和 $s_2+1$ 的方法数

$$\binom{b}{s_1-1-a}=\binom{b}{s_2+1-a},$$

因为后者的和接近 $b/2$. ■

定理 16.1 的条件的充分性是定理 16.2 的一个显而易见的推论. 如果 $\boldsymbol{r}^*$ 强于 $\boldsymbol{s}$，则

$$M(\boldsymbol{r},\boldsymbol{s})\geqslant M(\boldsymbol{r},\boldsymbol{r}^*)\geqslant 1.$$

**问题 16B** 证明 $M(\boldsymbol{r}, \boldsymbol{r}^*)=1$.

我们用 $A(n, k)$ 表示 $n\times n$(0，1)-矩阵中所有直线和等于 $k$ 的矩阵的数目.

**推论**

$$A(n,k)\geqslant\left\{\binom{n}{k}/2^{k+1}\right\}^n.$$

**证明** 行和为 $(k, k, \cdots, k)$ 的(0，1)-矩阵的数目是 $\binom{n}{k}^n$. 每一个矩阵有一个列和 $\boldsymbol{s}=(s_1, s_2, s_3, \cdots, s_n)$ 满足 $0\leqslant s_i\leqslant n$，$s_1+\cdots+s_n=nk$. 忽略限制 $s_i\leqslant n$，由定理 13.1 可以看到至多有 $\binom{nk+n-1}{n-1}\leqslant 2^{n(k+1)}$ 个这样的列和. 因为相联系的(0，1)-矩阵的最大数目出现于列和

$(k, k, \cdots, k)$，所以这样的矩阵的数目至少是平均数. ■

**问题 16C** 证明下面的定理.

**定理 16.3** *设 $\boldsymbol{d}$ 和 $\boldsymbol{d}'$ 是一个(偶)整数 $N$ 的两个分拆. 如果 $\boldsymbol{d}$ 强于 $\boldsymbol{d}'$，则以次数序列 $\boldsymbol{d}'$ 标号的简单图至少与以次数序列 $\boldsymbol{d}$ 标号的简单图一样多.*

**问题 16D** 如果 $n$ 是偶数，则

$$A\left(n, \frac{1}{2}n\right) \geqslant \frac{2^{n^2}}{n^{2n}}.$$

修改定理 16.2 的推论的证明来证明此式. $\left(\text{在那个推论中将 } k=\frac{1}{2}n \text{ 代入会给出一个不好的结果.}\right)$

**问题 16E** 设 $\boldsymbol{d}=(d_1, d_2, \cdots, d_n)$ 是 $\binom{n}{2}$ 的一个分拆(可能含有 0). 证明：存在顶点集 1，2，…，$n$ 上的一个竞赛图($K_n$ 的一个定向)使得对所有的 $i$ 顶点 $i$ 的出次为 $d_i$，当且仅当 [174]

$$(n-1, n-2, \cdots, 2, 1, 0)$$

强于 $\boldsymbol{d}$.

**问题 16F** (i)给定一个整数 $m \leqslant \binom{n}{2}$，考虑顶点集为 1，2，…，$n$ 的图，它的边是按照字典序的前 $m$ 个二元子集：

$$\{1,2\},\{1,3\},\cdots,\{1,n\},\{2,3\},\{2,4\},\cdots\{2,n\},\{3,4\},\cdots.$$

这个图有一个特定的次序列 $\boldsymbol{r}$，它是 $2m$ 的一个分拆. 例如，当 $n=8$ 且 $m=20$ 时，$\boldsymbol{r}=(7, 7, 7, 5, 4, 4, 3, 3)$. 给定 $n$，$m \leqslant \binom{n}{2}$，以及 $2m$ 的一个分拆 $\boldsymbol{d}$(可能包括 0)，证明：在 $n$ 个顶点上有一个次序列为 $\boldsymbol{d}$ 的简单图，当且仅当上面描述的分拆 $\boldsymbol{r}$ 强于 $\boldsymbol{d}$.

(ii)推广到简单的 $k$-均匀超图(一个点集和 $k$ 元子集的集合).

* * *

如在第 11 章中那样，设 $\mathcal{A}(n, 2)$ 表示大小为 $n$ 且所有直线和等于 2 的(0，1)-矩阵. 利用第 14 章讲过的一个方法对 $\mathcal{A}(n, 2)$ 中元素的数目 $A(n, 2)$ 计数.

设 $\mathcal{A}^*(n, 2)$ 表示 $\mathcal{A}(n, 2)$ 的由不可分解的矩阵(参见第 11 章)构成的子集. 定义 $a_n := |\mathcal{A}^*(n, 2)|$. 按照下面的方式容易看出 $a_n = \frac{1}{2}n!\,(n-1)!$. 对第一行我们有 $\binom{n}{2}$ 种选择. 如果选择(1 1 0…0)作为第一行，那么还有(其余 $n-1$ 行中)一行在第一列是 1 并且另一个 1 不在第二列(因此有 $n-2$ 种选择). 这给出 $(n-1)(n-2)$ 种可能，等等.

现在定义

$$m_n := A(n,2)/(n!)^2,$$

$$b_k := a_k/(k!)^2.$$ [175]

那么由定理 14.2 中所用的相同的论证，我们有

$$1 + \sum_{n=2}^{\infty} m_n x^n = \exp\left(\sum_{k=2}^{\infty} b_k x^k\right). \tag{16.1}$$

所以，我们得到

$$1+\sum_{n=2}^{\infty}m_n x^n=\exp\left(\frac{-x-\log(1-x)}{2}\right)=\mathrm{e}^{-\frac{1}{2}x}(1-x)^{-\frac{1}{2}}. \tag{16.2}$$

从展开式

$$(1-x)^{-\frac{1}{2}}=\sum_{n=0}^{\infty}\binom{2n}{n}\left(\frac{x}{4}\right)^n$$

证明(16.2)是很容易的，我们断定

$$m_n\sim \mathrm{e}^{-\frac{1}{2}}\binom{2n}{n}4^{-n}\quad 对\ n\to\infty.$$

因此，我们已经证明了下面的定理.

**定理 16.4**

$$A(n,2)\sim \mathrm{e}^{-\frac{1}{2}}\frac{(2n)!}{(2!)^{2n}}.$$

这个定理又是如下定理的特殊情形(我们仅对 $k=3$ 加以证明，所用的方法可用于 $k$ 的其他值).

**定理 16.5**

$$A(n,k)=\frac{(nk)!}{(k!)^{2n}}\exp\left[-\frac{(k-1)^2}{2}\right]\left\{1+O\left(\frac{1}{n^{\frac{3}{4}}}\right)\right\}\qquad(n\to\infty),$$

当 $1\leqslant k<\log n$ 时，对 $k$ 一致成立.

对这个问题的更多信息以及在直线和不是常数时的推广，可参考 B. D. McKay(1984).

对 $k=3$ 的情形，现在我们证明一个比在上式中置 $k=3$ 所得到的稍强的结果. 我们利用容斥原理的截断形式(参见定理 10.1 的注记).

考虑 $N:=3n$ 个元素，编号为

$$1_a,1_b,1_c,2_a,2_b,2_c,\cdots,n_a,n_b,n_c.$$

这 $N$ 个元素组成一个排列，然后按对应的顺序划分成三元组：$(x,\ y,\ z)(u,\ v,\ w)\cdots$. 如果这些三元组中至少有一组，某个数的出现多于一次，如在$(5_a,\ 3_b,\ 5_c)$中，我们说发生了一次重复. 假设所选的排列产生的 $n$ 个三元组中没有重复. 在这种情形，我们把一个 $n\times n$ (0, 1)-矩阵与这个排列如下关联：如果第 $i$ 个三元组是$(x_\alpha,\ y_\beta,\ z_\gamma)$，其中$\{\alpha,\ \beta,\ \gamma\}\subseteq\{a,\ b,\ c\}$，则矩阵中行 $i$ 的 $x$，$y$，$z$ 列是 1，在其余的地方是 0. 因为指标 $a$，$b$，$c$ 不影响矩阵，一个三元组中三个元素的顺序也是不相关的，所以每一个这样的矩阵对应$(3!)^{2n}$个不同的排列. 显然，这样的矩阵在$A(n,\ 3)$中. 在 $3n$ 个元素的所有 $N_0:=N!$ 个排列中没有重复的排列的数目为 $P$，我们必须找到 $P$ 的一个估计.

设 $1\leqslant r\leqslant n$. 指定 $r$ 个三元组并对在这些三元组中有一个重复的排列计数. 然后对 $r$ 个三元组的所有选择求和，如同在定理 10.1 中，我们称这个数为 $N_r$，那么，如果 $r$ 是偶数，我们有

$$\sum_{r=0}^{R+1}(-1)^r N_r\leqslant P\leqslant\sum_{r=0}^{R}(-1)^r N_r. \tag{16.3}$$

证明的困难的部分是寻找 $N_r$ 的适当的上界估计和下界估计.

我们从上界估计开始. 有 $\binom{n}{r}$ 种方式选择 $r$ 个三元组. 在每个三元组中指定两个位置，在那里要求有一次重复. 这可由 $3^r$ 种方式完成. 现在选择 $r$ 个数，以及指标 $a$，$b$，$c$ 出现在重复中，这也有 $\binom{n}{r}\cdot 3^r$ 种方式. 然后，把已选择的数分配到已选择的位置上，这可由 $2^r\cdot r!$ 种方式完成. 最后，随意地分配其余的 $N-2r$ 个数. 显然，有类型为$(5_a,\ 5_b,\ 5_c)$重复的排列在计数时被计算了超过一次. 于是，我们有 177

$$
\begin{aligned}
N_r &\leqslant \binom{n}{r}^2\cdot 3^{2r}\cdot 2^r\cdot r!\cdot(N-2r)! \\
&\leqslant \frac{2^r}{r!}(3^2\cdot n^2)^r(N-2r)!\leqslant N!\frac{2^r}{r!}\left(\frac{N-2r}{N}\right)^{-2r} \\
&\leqslant N!\frac{2^r}{r!}\left(1+\frac{8r^2}{N}\right),
\end{aligned}
\tag{16.4}
$$

如果 $r<\frac{1}{2}\sqrt{n}$. 这里，最后一步基于 $\left(1-\frac{2r}{N}\right)^{-2r}$ 的幂级数展开，并这样选择 $r$，使每一项至多是前一项的一半.

对下界估计，我们以同样的方式开始. 在 $r$ 对已经选出并分配到选择了的位置之后，首先我们填满 $r$ 个有一次重复的三元组，在每个三元组中使用与重复的数不同的数. 显然，这能用 $(N-3r)^r$ 种不同的方法来完成. 然后我们分配其余的数. 有些应该计数的排列没有被计数，即

$$
\begin{aligned}
N_r &\geqslant \binom{n}{r}^2\cdot 3^{2r}\cdot 2^r\cdot r!\cdot(N-3r)^r(N-3r)! \\
&\geqslant N!\frac{2^r}{r!}(3^2\cdot n^2)^r\left[\frac{n(n-1)\cdots(n-r+1)}{n^r}\right]^2\frac{(N-3r)^r}{N^{3r}} \\
&\geqslant N!\frac{2^r}{r!}\left(1-\frac{r}{n}\right)^{2r}\left(1-\frac{3r}{N}\right)^r \\
&\geqslant N!\frac{2^r}{r!}\left(1-\frac{3r^2}{n}\right),
\end{aligned}
\tag{16.5}
$$

如果 $r<\sqrt{n}$. 这里，最后一步使用了众所众知的不等式

$$\left(1-\frac{r}{n}\right)^r\geqslant 1-\frac{r^2}{n},\quad 如果\ 1\leqslant r\leqslant\sqrt{n}.$$ 178

现在我们把(16.3)、(16.4)和(16.5)结合起来. 取 $R=\left\lfloor\frac{1}{2}\sqrt{n}\right\rfloor$. 我们发现

$$\frac{P}{N!}=\mathrm{e}^{-2}+\Delta,\quad 其中\quad |\Delta|<\frac{2^{R+1}}{(R+1)!}+\frac{3}{n}\sum_{r=0}^{\infty}\frac{2^r r^2}{r!},$$

且因此

$$|\Delta|<\frac{48}{n}+\frac{18\mathrm{e}^2}{n}<\frac{200}{n}.$$

所以，我们已经发现了如下的估计(与定理 16.5 相符).

**定理 16.6** 我们有

$$A(n,3)=\frac{(3n)!}{(3!)^{2n}}e^{-2}\left(1+O\left(\frac{1}{n}\right)\right)\quad(n\to\infty).$$

**注记** 注意，对 $k=3$，从定理 16.2 的推论我们发现对某个适当的常数 $c$，$A(n, 3)$增长得与$(cn^3)^n$ 一样快，这与定理 16.6 仅差一个常数.

**问题 16G** 确定 $A(5, 3)$.

现在我们描述(16.2)和第 14 章之间的联系. 注意到(16.2)的右边的平方产生更列排列数的指数生成函数，更列排列数在例 14.10 中给出. 这意味着我们应能组合地证明

$$n!d_n=\sum_{k=0}^{n}\binom{n}{k}^2A_kA_{n-k},\tag{16.6}$$

这里我们用 $A_n$ 代替 $A(n, 2)$.

作为准备，考虑$\mathcal{A}(n, 2)$的一个元素的不可分解分量，例如如下的 $n=9$ 时的 $5\times5$ 子矩阵：

| | 1 | 3 | 4 | 5 | 9 |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 |
| 2 | 1 | 0 | 1 | 0 | 0 |
| 3 | 0 | 1 | 0 | 0 | 1 |
| 7 | 0 | 0 | 1 | 1 | 0 |
| 9 | 0 | 0 | 0 | 1 | 1 |

179

从第一行的两个 1 开始，有两种方式描述对应于行的排列(1 3 9 7 2)的循环结构：

$$(1,3),(3,9),(9,5),(5,4),(4,1)$$

以及对应于逆排列(1 2 7 9 3)的循环结构：

$$(3,1),(1,4),(4,5),(5,9),(9,3).$$

第一种情形($1<3$)我们称为红簇，第二种情形为蓝簇.

考虑由$\mathcal{A}(n, 2)$中的元素组成的集合 $S$，每个元素中的 1 染成红的或蓝的，使得在一个不可分解分量中所有的 1 有相同的颜色. 显然

$$|S|=\sum_{k=0}^{n}\binom{n}{k}^2A_kA_{n-k}.$$

我们定义从 $S$ 到 1，2，…，$n$ 的排列对$(a_1, a_2, \cdots, a_n)$，$(b_1, b_2, \cdots, b_n)$的一个一一映射，排列对中的第一个是更列排列 . 有 $n!\ d_n$ 个这样的排列对. 我们通过例子做到这一点.

设

$$a:=(a_1,a_2,\cdots,a_9)=(2,7,1,8,4,5,9,6,3),$$
$$b:=(b_1,b_2,\cdots,b_9)=(3,1,4,5,9,2,6,8,7).$$

$a$ 的标准圈分解是(1 2 7 9 3)(4 8 6 5). 相应地我们把 $b$ 分裂成(3 1 4 5 9)和(2 6 8 7). 第一个排列对描述了上面处理过的 5×5 蓝子矩阵；第二个排列对描述了一个 4×4 红子矩阵 .

这就建立了(16.6).

下面的问题给出了另一个与第 14 章的关系.

**问题 16H** 再次设 $A_n:=A(n,2)$. 考虑$\mathcal{A}(n,2)$中的一个矩阵. 在第一行选择两个 1 有$\binom{n}{2}$种方法. 假设这两个 1 在前两列. 其他行也可能有两个 1 在前两列. 现在，考虑其他可能性并证明 [180]

$$A_n=\frac{n(n-1)}{2}(2A_{n-1}+(n-1)A_{n-2}). \tag{16.7}$$

**问题 16I** 设 $f(x)$是(16.1)的左边定义的函数. 从(16.7)导出微分方程

$$2(1-x)f'-xf=0$$

并给出(16.2)的第二个证明.

## 评注

定理 16.1 属于 D. Gale(1957)和 H. J. Ryser(1957). 我们考虑过的对(0，1)-矩阵类的更为广泛的处理，参照了 Ryser(1963).

(16.2)和更列排列的生成函数之间的联系由 D. G. E. D. Rogers 向我们指出. (16.6)的证明属于 P. Diaconis 和 D. E. Knuth(私人通信).

关系式(16.7)由 R. Bricard(1901)给出，但没有证明.

## 参考文献


R. Bricard (1901), Problème de combinaisons, *L'Intermédiaire des Mathématiciens* **8**, 312–313.

D. Gale (1957), A theorem on flows in networks, *Pacific J. Math.* **7**, 1073–1082.

M. Krause (1996), A simple proof of the Gale-Ryser theorem, *Amer. Math. Monthly* **103**, 335–337.

B. D. McKay (1984), Asymptotics for (0,1)-matrices with prescribed line sums, in: *Enumeration and Design* (D. M. Jackson and S. A. Vanstone, eds.), Academic Press.

H. J. Ryser (1957), Combinatorial properties of matrices of zeros and ones, *Canad. J. Math.* **9**, 371–377.

H. J. Ryser (1963), *Combinatorial Mathematics*, Carus Math. Monograph **14**. [181]

# 第17章 拉 丁 方

一个 $n$ 阶拉丁方是一个四元组 $(R, C, S; L)$，这里 $R$，$C$ 和 $S$ 是基数为 $n$ 的集合，$L$ 是映射 $L: R\times C\to S$，使得对任意的 $i\in R$ 和 $x\in S$，方程

$$L(i,j) = x$$

有唯一解 $j\in C$；且对任意的 $j\in C$，$x\in S$，同一个方程有唯一解 $i\in R$. 这就是，$i\in R$，$j\in C$，$x\in S$ 中的任意两个唯一地确定第三个，使得 $L(i, j)=x$. $R$ 中的元素称为行，$C$ 中的元素称为列，$S$ 中的元素称为拉丁方的符号或项. 一个拉丁方通常写成 $n\times n$ 的阵列，在第 $i$ 行第 $j$ 列的腔中包含符号 $L(i, j)$. 图 17.1 给出了 5 阶拉丁方的一个例子.

术语"拉丁方"源自欧拉，他用拉丁字母表示 $S$.

| a | b | c | d | e |
|---|---|---|---|---|
| b | a | e | c | d |
| c | d | b | e | a |
| d | e | a | b | c |
| e | c | d | a | b |

图 17.1

拟群是有相同的行、列以及符号集 $X$ 的一个拉丁方 $(X, X, X; \circ)$. 这里我们把四元组表示的拟群简写成 $(X, \circ)$. 现在，映射 $\circ$



是 $X$ 上的一个二元运算，并且在 $\circ$ 下 $(x, y)$ 的象用 $x\circ y$ 表示. 于是，作为一种特殊情况，我们得到群的乘法表的拉丁方.

**问题 17A** 在图 17.1 中，如果固定前两行，那么有许多种方法填充其余的三行以得到一个拉丁方(事实上有 24 种方法). 证明这些拉丁方中没有一个是一个群的乘法表.

注意，如果 $(R, C, S; L)$ 是一个拉丁方，映射 $\sigma: R\to R'$，$\tau: C\to C'$，$\pi: S\to S'$ 是双射，而且如果我们定义 $L'(\sigma(i), \tau(j)) := \pi(L(i, j))$，那么 $(R', C', S'; L')$ 是一个拉丁方. 这两个拉丁方称为等价的. 由等价性的概念，可以假设在整数集 $S:=\{1, 2, \cdots, n\}$ 上的一个拉丁方按从 1 到 $n$ 的顺序既作为它的第一行又作为它的第一列. 注意按这种方式标准化的两个不同的拉丁方，仍可能是等价的.

有时我们只用"$L: R\times C\to S$"表示一个拉丁方.

阶为 $n$ 且深度为 3 的正交阵列 $OA(n, 3)$ 是以从 1 到 $n$ 的整数作为项的一个 $3\times n^2$ 阵列，使得对阵列的任意两行，在这些行中出现的 $n^2$ 个竖直方向的对子是不同的. 假定我们有一个这样的阵列. 按任意的顺序称呼行 $\boldsymbol{r}$，$\boldsymbol{c}$ 和 $\boldsymbol{s}$. 对任意的对子 $(i, j)$，存在一个 $k$ 使得 $r_k=i$，$c_k=j$. 我们以在 $i$ 行和 $j$ 列(对所有的 $i, j$)的项 $s_k$ 作一个正方形. 正交阵列的定义保证这是一个拉丁方而且可以把过程反过来. 所以，拉丁方和正交阵列的概念是等价的. 图 17.2 显示一个 $OA(4, 3)$ 和对应的两个拉丁方.

| 行 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 3 | 3 | 3 | 3 | 4 | 4 | 4 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 列 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 符号 | 3 | 2 | 4 | 1 | 1 | 4 | 2 | 3 | 4 | 3 | 1 | 2 | 2 | 1 | 3 | 4 |

| 3 | 2 | 4 | 1 |
|---|---|---|---|
| 1 | 4 | 2 | 3 |
| 4 | 3 | 1 | 2 |
| 2 | 1 | 3 | 4 |

| 符号 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 3 | 3 | 3 | 3 | 4 | 4 | 4 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 列 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 行 | 3 | 2 | 4 | 1 | 1 | 4 | 2 | 3 | 4 | 3 | 1 | 2 | 2 | 1 | 3 | 4 |

| 2 | 4 | 3 | 1 |
|---|---|---|---|
| 4 | 1 | 2 | 3 |
| 1 | 3 | 4 | 2 |
| 3 | 2 | 1 | 4 |

图 17.2

与有相同的三行(可能按照不同的顺序)的正交阵列对应的两个拉丁方称为共轭拉丁方. 例如，一个拉丁方(其中 $R=C$)的共轭是它的转置. 作为一个练习，读者应能写出图 17.2 中拉丁方的六个共轭. 两个正交阵列称为是同构的，如果一个阵列能从另一个阵列通过其每一行元素的排列以及阵列的行和列的排列得到. 与同构的正交阵列对应的两个拉丁方也称为是同构的. 这意味着其中的一个与另一个的共轭等价.

**问题 17B** 通过分别设 $a=1$，$b=2$ 和 $a=2$，$b=1$，考虑从图 17.3 得到的两个拉丁方. 证明这两个拉丁方是等价的. 证明与这些拉丁方不等价的一个拉丁方和 5 阶循环群对应.

可以把拉丁方解释为一个三维 0 和 1 的阵列，在与其中一边平行的阵列的每条线上恰有一个 1. 例如，在图 17.3 中，第 2 行第 3 列的项 4 应解释成在阵列的位置(2，3，4)的项 1.

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 2 | 1 | 4 | 5 | 3 |
| 3 | 5 | a | b | 4 |
| 4 | 3 | 5 | a | b |
| 5 | 4 | b | 3 | a |

图　17.3

下一章我们将考虑深度大于 3 的正交阵列. 构建它们常常要比构建阵列 $OA(n, 3)$难得多.

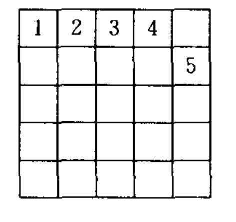
**问题 17C** 构建一个 $OA(4, 4)$，即项为 1，2，3，4 的 $4\times16$ 矩阵 $A$，使得对 $A$ 的任意两行，比如说第 $i$ 行和第 $j$ 行，16 个对子$(a_{ik}, a_{jk})$ $(1\leqslant k\leqslant16)$全不相同.

183
~
184

拉丁方$(R, C, S; L)$的一个子拉丁方是$(R_1, C_1, S_1; L_1)$，满足对$(i, j)\in R_1\times C_1$ 有 $R_1\subseteq R$，$C_1\subseteq C$，$S_1\subseteq S$，且 $L_1(i, j)=L(i, j)$.

**问题 17D** 设 $m$ 和 $n$ 是正整数，$m<n$，证明：存在一个包含 $m$ 阶子拉丁方的 $n$ 阶拉丁方的充要条件是 $m\leqslant\frac{1}{2}n$.

下面的问题都有一个类似的性质. 它们关心的问题类似于问题 17B 和 17D 的情况，即完成已部分被填充的一个拉丁方. 一个 $n\times n$ 的阵列 $A$ 称为部分拉丁方，如果它的腔或者是空或者恰包含一个符号，而且没有一个符号在任何一行或一列出现超过一次. (说阵列"有拉丁方性质"可能更好，但我们将使用以前的术语.)我们对保证部分拉丁方被补足成一个 $n$ 阶拉丁方的条件感兴趣，即何时空的腔填上符号以得到一个拉丁方. 例如，如果 $A$ 是一个除了最后一行其他的腔都被填满(即非空)的部分拉丁方，显然有唯一一种方法把 $A$ 补足成一个拉丁方. 另一方面，图 17.4 中的两个部分拉丁方显然不能被补足.



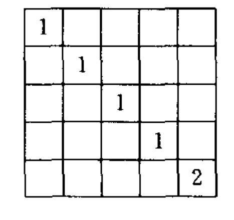



图　17.4

185

通过只考虑已填充的腔，我们可以把部分拉丁方与一个阵列相联系，方法与对拉丁方所做的相同. 这允许我们定义一个部分拉丁方的共轭. 在图 17.4 中，两个部分拉丁方实际上并不是在本质上不同，而是共轭，从下面所显示的部分 $OA(5, 3)$来看是显然的：

$$\begin{matrix}\text{行}\\ \text{列}\\ \text{符号}\end{matrix}\quad\begin{bmatrix}1&1&1&1&2\\1&2&3&4&5\\1&2&3&4&5\end{bmatrix}\quad\begin{bmatrix}1&2&3&4&5\\1&2&3&4&5\\1&1&1&1&2\end{bmatrix}$$

如果一个部分拉丁方的前 $k$ $(k\leqslant n)$行被填充而且其余的腔空着，则 $A$ 称为 $k\times n$ 拉丁

矩形.

**定理 17.1** 一个 $k\times n(k<n)$ 的拉丁矩形，可以扩展为 $(k+1)\times n$ 的拉丁矩形(且因此它能被补足).

**证明** 设 $B_j$ 表示没有出现在 $A$ 的列 $j$ 的正整数集合，从 1 到 $n$ 的每个数字在 $A$ 中出现 $k$ 次，所以在诸集合 $B_j$ 中出现 $n-k$ 次. 诸集合 $B_j$ 中的任意 $l$ 个一起包含 $l(n-k)$ 个元素，所以至少有 $l$ 个互不相同. 于是集合 $B_j(1\leqslant j\leqslant n)$ 有第 5 章的性质 $H$，且由定理 5.1，它们有一个 SDR. 这个 SDR 可以作为第 $(k+1)$ 行邻接在 $k\times n$ 的拉丁矩形上. ■

我们用 $L(n)$ 表示不同的 $n$ 阶拉丁方的总数. 现在仅知道 $n\leqslant 9$ 时的 $L(n)$ 的准确值. 拉丁方的数目增加得非常快速，尽管有两个不等价的 5 阶拉丁方，但是有 5! ·4! ·56 个不同的 5 阶拉丁方.

**定理 17.2** $L(n)\geqslant (n!)^{2n}/n^{n^2}$.

**证明** 为了构造一个 $n$ 阶拉丁方，可以取 1 到 $n$ 的任何一个排列作为它的第一行. 如果已构造了一个 $k$ 行的拉丁矩形，则由定理 17.1 的证明，选择下一行的方法数是 per $B$，这里 $b_{ij}=1$，如果 $i\in B_j$. 由定理 12.8(范德瓦尔登猜想)这个积和式至少为 $(n-k)^n\cdot n!/n^n$，于是我们发现

186

$$L(n)\geqslant n!\prod_{k=1}^{n-1}\{(n-k)^n n!/n^n\}=(n!)^{2n}/n^{n^2}. \tag{17.1}$$

■

**注记** 如果利用定理 5.3，我们就会发现估计 $L(n)\geqslant n!\,(n-1)!\cdots 1!$ (H. J. Ryser, 1969)，与(17.11)相比，它在 $n$ 小时较好，但渐近地要比(17.1)小得多.

对 $n=8$，估计(17.1)小于真实值乘以 $10^{-4}$，但渐近地(17.1)是最佳可能的，正如下个定理所示.

**定理 17.3** 如果定义 $\mathcal{L}(n):=\{L(n)\}^{1/n^2}$，则

$$\mathcal{L}(n)\sim e^{-2}n \quad 对\ n\to\infty.$$

**证明** 从(17.1)和斯特林公式，我们发现 $n^{-1}\mathcal{L}(n)\geqslant e^{-2}$. 利用与定理 17.2 的证明中相同的论证，又通过用定理 11.5 估计 per $B$，我们发现

$$L(n)\leqslant\prod_{k=1}^{n}M(n,k)\leqslant\prod_{k=1}^{n}(k!)^{n/k}.$$

因此，再次由带某个大于$\sqrt{2\pi}$的常数 $C$ 的斯特林公式，我们有

$$\begin{aligned}\log\mathcal{L}(n)&\leqslant\frac{1}{n}\sum_{k=1}^{n}\frac{1}{k}\log k!\\&\leqslant\frac{1}{n}\sum_{k=1}^{n}\left\{\log k-1+\frac{1}{2k}\log k+\frac{1}{k}\log C\right\}\\&=\frac{1}{n}\sum_{k=1}^{n}\log k-1+o(1)\end{aligned}$$

$$= -2 + \log n + o(1) \quad 对\ n \to \infty.$$

把这个界与下界结合，我们得到要求的结果. ■

下面属于 H. J. Ryser(1951)的定理是问题 17D 的一个推广.

**定理 17.4** 设 $A$ 是阶为 $n$ 的一个部分拉丁方，其中腔$(i, j)$被填充，当且仅当 $i \leqslant r$ 且 $j \leqslant s$. 则 $A$ 能被补足，当且仅当对 $i=1, \cdots, n$，$N(i) \geqslant r+s-n$，这里 $N(i)$表示 $A$ 中等于 $i$ 的元素的数目.

187

**证明** 首先，观察在一个 $n$ 阶的拉丁方中，前 $r$ 行恰好包含 $r$ 个等于 $i$ 的元素，其中至多 $n-s$ 个元素在最后的 $n-s$ 列. 于是加在 $N(i)$上的条件的必要性是平凡的. 我们来证明这个条件也是充分的. 设 $B$ 是大小为 $r \times n$ 的(0, 1)-矩阵，满足 $b_{ij}=1$ 当且仅当元素 $j$ 不出现在 $A$ 中的行 $i$. 显然，$B$ 的每一行有和$(n-s)$. $B$ 的第 $j$ 列有和 $r-N(j) \leqslant n-s$. 由定理 7.5($d := n-s$)我们有

$$B = L^{(s+1)} + \cdots + L^{(n)},$$

这里 $L^{(i)}$是每一行有一个 1 且每一列至多有一个 1 的 $r \times n$ 的(0, 1)-矩阵.

作为一个例子，假设 $r=s=4$，$n=7$，$A$ 的前四行是

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | | | |
| 5 | 3 | 1 | 6 | | | |
| 3 | 1 | 5 | 2 | | | |
| 7 | 4 | 2 | 5 | | | |

则

$$B := \begin{bmatrix} 0&0&0&0&1&1&1 \\ 0&1&0&1&0&0&1 \\ 0&0&0&1&0&1&1 \\ 1&0&1&0&0&1&0 \end{bmatrix} = L^{(5)} + L^{(6)} + L^{(7)}$$

$$= \begin{bmatrix} 0&0&0&0&0&0&1 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0 \end{bmatrix} + \begin{bmatrix} 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \\ 0&0&0&1&0&0&0 \\ 0&0&1&0&0&0&0 \end{bmatrix} + \begin{bmatrix} 0&0&0&0&1&0&0 \\ 0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&0 \end{bmatrix}.$$

比如说，$L^{(t)} = [l_{ij}^{(t)}]$. 那么，如果 $l_{ik}^{(j)}=1$，我们将 $A$ 的位置$(i, j)$的腔填上 $k$，其中 $i=1, \cdots, r$，$j=s+1, \cdots, n$. 在我们的例子中，用

| 7 |
|---|
| 4 |
| 6 |
| 1 |

，

| 6 |
|---|
| 7 |
| 4 |
| 3 |

，

| 5 |
|---|
| 2 |
| 7 |
| 6 |

188

来填充后三列. 于是 $A$ 变成 $r$ 行填满的一个 $n$ 阶部分拉丁方，即一个拉丁矩形. 由定理 17.1，这个矩形可以被补足为一个阶为 $n$ 的拉丁方. ■

图 17.4 中两个已填上 $n$ 个腔的部分拉丁方，是不能被补足为拉丁方的例子．一个少于 $n$ 个腔被填充的部分拉丁方能补足为一个拉丁方的猜想，在它最终被 B. Smetaniuk(1981)证明之前，作为 Evans 猜想而知名．也许 Smetaniuk 的证明中最重要的部分是定理 17.5 的构造．

**定理 17.5** 设 $A$ 是一个 $n$ 阶拉丁方．设 $B$ 是一个$(n+1)\times(n+1)$的阵列，对 $i$，$j\geqslant1$，$i+j\leqslant n+1$，它的$(i, j)$项是 $A$ 的$(i, j)$项，它有一个新的符号 $\alpha$ 在反对角线上，反对角线之下的腔是空的，那么 $B$ 能被补足为一个阶为 $n+1$ 的拉丁方．

5 阶拉丁方 $A$ 和它所对应的阵列 $B$ 的一个例子如下所示．

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 4 | 3 | 5 | 1 | 2 |
| 2 | 5 | 1 | 3 | 4 |
| 5 | 1 | 4 | 2 | 3 |
| 3 | 4 | 2 | 5 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | α |
| 4 | 3 | 5 | 1 | α | |
| 2 | 5 | 1 | α | | |
| 5 | 1 | α | | | |
| 3 | α | | | | |
| α | | | | | |

**证明** 设 $C$ 是 $B$ 通过去掉最后一行和最后一列而得到的 $n\times n$ 阵列．在我们的例子中，$C$ 是下面的阵列．

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 4 | 3 | 5 | 1 | α |
| 2 | 5 | 1 | α | |
| 5 | 1 | α | | |
| 3 | α | | | |

我们描述一个算法，由这个算法在满足前 $r$ 行被填满的限制下，一行接一行地填充 $C$ 的空腔，我们将得到一个有 $n+1$ 个符号 1，2，…，$n$，$\alpha$ 的 $r\times n$ 的拉丁矩形，使得第 $j$ 列按某一顺序与 $A$ 的前 $r$ 行包含相同的符号，但包含 $x$ 的每一列中那个所谓的“缺失的”符号除外，并且使得 $r-1$ 个缺失的符号各不相同．这对 $r=1$ 和 $r=2$ 是平凡的．假设对某个 $r(2\leqslant r<n)$ 已实施算法，并且此时缺失的符号为

[189]

$$x_{n-r+2}, x_{n-r+3}, \cdots, x_n.$$

为了填充第$(r+1)$行，我们如下进行．

设 $A$ 在列 $r+1$ 中的最后 $r$ 个符号(它们在构造 $C$ 时已被移去)是

$$y_{n-r+1}, y_{n-r+2}, y_{n-r+3}, \cdots, y_n.$$

这里 $y_{n-r+1}$ 是被 $\alpha$ 替换掉的符号，并且在这一列中是新的缺失的元素．我们可以考虑用

$$y_{n-r+2}, y_{n-r+3}, \cdots, y_n$$

填充行 $r+1$，而且这被满足，如果

$$y_{n-r+1}, x_{n-r+2}, x_{n-r+3}, \cdots, x_n$$

(它们是新的缺失的符号)是不同的．否则，考虑序列

$$y_{n-r+1} = x_{k_1}$$
$$y_{k_1} = x_{k_2}$$
$$\vdots$$
$$y_{k_{m-1}} = x_{k_m}$$

扩展到使得 $y_{k_m}$ 不等于任何一个 $x_j$. 然后，我们用 $y_{n-r+2}$，$y_{n-r+3}$，…，$y_n$ 填充 $r+1$ 行，除非 $y_{k_1}$，$y_{k_2}$，…，$y_{k_m}$ 被略去且分别被 $x_{k_1}$，$x_{k_2}$，…，$x_{k_m}$ 替换. 必须检查整个行 $r+1$ 以确保它含有不同的符号. 新的缺失的符号是 $y_{n-r+1}$ 和 $x_{n-r+2}$，$x_{n-r+3}$，…，$x_n$，除非 $x_{k_1}$，$x_{k_2}$，…，$x_{k_m}$ 被略去且分别被 $y_{k_1}$，$y_{k_2}$，…，$y_{k_m}$ 代替，必须检查这些符号是各不相同的. [190]

一旦 $C$ 的空腔被填充，$B$ 的最后一行的前 $n$ 个空腔即被 $x$ 和缺失的符号填充(当 $r=n$ 时). 我们现在有一个$(n+1)\times n$ 的拉丁矩形，它唯一地被补足成一个 $n+1$ 阶拉丁方. ■

**问题 17E** 设 $A$ 表示左下方的阶为 10 的拉丁方，并且设 $C$ 是右下方有 11 个符号 0，1，2，…，9，$\alpha$ 的部分的 10×10 拉丁矩形(不包括最后一行以及最后一列). 利用定理 17.5 的证明中的算法，补足 $C$ 为符号是 0，1，2，…，9，$\alpha$ 的 10×10 的拉丁矩形. 然后把这个拉丁矩形补足成一个阶为 11 的拉丁方.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 3 | 5 | 9 | 6 | 0 | 2 | 8 | 7 |
| 5 | 8 | 9 | 2 | 6 | 7 | 3 | 4 | 1 | 0 |
| 9 | 4 | 5 | 6 | 0 | 3 | 7 | 8 | 2 | 1 |
| 1 | 3 | 4 | 7 | 5 | 2 | 8 | 9 | 0 | 6 |
| 2 | 6 | 1 | 3 | 7 | 4 | 5 | 0 | 9 | 8 |
| 7 | 9 | 0 | 1 | 4 | 8 | 2 | 3 | 6 | 5 |
| 6 | 7 | 8 | 9 | 1 | 0 | 4 | 5 | 3 | 2 |
| 8 | 5 | 6 | 0 | 2 | 9 | 1 | 7 | 4 | 3 |
| 3 | 0 | 2 | 4 | 8 | 5 | 6 | 1 | 7 | 9 |
| 0 | 2 | 7 | 8 | 3 | 1 | 9 | 6 | 5 | 4 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 3 | 5 | 9 | 6 | 0 | 2 | 8 | 7 | $\alpha$ |
| 5 | 8 | 9 | 2 | 6 | 7 | 3 | 4 | 1 | $\alpha$ | |
| 9 | 4 | 5 | 6 | 0 | 3 | 7 | 8 | $\alpha$ | | |
| 1 | 3 | 4 | 7 | 5 | 2 | 8 | $\alpha$ | | | |
| 2 | 6 | 1 | 3 | 7 | 4 | $\alpha$ | | | | |
| 7 | 9 | 0 | 1 | 4 | $\alpha$ | | | | | |
| 6 | 7 | 8 | 9 | $\alpha$ | | | | | | |
| 8 | 5 | 6 | $\alpha$ | | | | | | | |
| 3 | 0 | $\alpha$ | | | | | | | | |
| 0 | $\alpha$ | | | | | | | | | |
| $\alpha$ | | | | | | | | | | |

(例如，用算法填充 $C$ 的前五行如右下图所示. 此时从第 7 列到第 10 列"缺失的"元素分别是 5，9，2，0. 现在考虑第 6 行. 第 6 列中的 $\alpha$ 迫使 8 成为第 6 列缺失的元素. 但 8 与目前从其他列缺失的元素不同. 于是这里不需再做什么；只需用来自 $A$ 中第 6 行的项 2，3，6，5 填充 $C$ 的第 6 行.) [191]

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 3 | 5 | 9 | 6 | 0 | 2 | 8 | 7 |
| 5 | 8 | 9 | 2 | 6 | 7 | 3 | 4 | 1 | 0 |
| 9 | 4 | 5 | 6 | 0 | 3 | 7 | 8 | 2 | 1 |
| 1 | 3 | 4 | 7 | 5 | 2 | 8 | 9 | 0 | 6 |
| 2 | 6 | 1 | 3 | 7 | 4 | 5 | 0 | 9 | 8 |
| 7 | 9 | 0 | 1 | 4 | 8 | 2 | 3 | 6 | 5 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 3 | 5 | 9 | 6 | 0 | 2 | 8 | 7 |
| 5 | 8 | 9 | 2 | 6 | 7 | 3 | 4 | 1 | $\alpha$ |
| 9 | 4 | 5 | 6 | 0 | 3 | 7 | 8 | $\alpha$ | 1 |
| 1 | 3 | 4 | 7 | 5 | 2 | 8 | $\alpha$ | 0 | 6 |
| 2 | 6 | 1 | 3 | 7 | 4 | $\alpha$ | 0 | 9 | 8 |
| 7 | 9 | 0 | 1 | 4 | $\alpha$ | | | | |

**问题 17F** (i)设 $A$ 和 $B$ 是符号为 1，2，…，$n$ 的 $n$ 阶拉丁方．设 $A'$ 和 $B'$ 是符号为 1，2，…，$n+1$ 的拉丁方($n+1$ 在它们的反对角线上)，在反对角线上方，它们分别与 $A$ 和 $B$ 一致，如在定理 17.5 的证明中所构造的．证明：如果 $A$ 和 $B$ 是不同的，则 $A'$ 和 $B'$ 也是不同的．这证明 $n+1$ 在反对角线上的 $n+1$ 阶拉丁方的数目大于或等于 $n$ 阶拉丁方的数目 $N(n)$．

(ii)解释(i)怎样导致在定理 17.2 后面的注记中提到的结果

$$L(n) \geqslant n!(n-1)!\cdots 2!1!.$$

**定理 17.6**　*一个至多有 $n-1$ 个腔被填充的 $n$ 阶部分拉丁方能被补足为一个 $n$ 阶拉丁方．*

**证明**　这一定理将用归纳法来证明．设它对 $n$ 成立，并且设 $L$ 是一个至多有 $n$ 个腔被填充的阶为 $n+1$ 的部分拉丁方．

首先，假设存在 $L$ 的一个符号 $x$，它仅在 $L$ 中出现一次．我们打算重排行和列使已被填充的腔移到反对角线之上，但单一符号 $x$ 在反对角线上除外．比如说有被填充的腔的行有 $f_1$，$f_2$，…，$f_k$ 个被填充的腔，这里 $f_1+\cdots+f_k \leqslant n$，且 $x$ 在有 $f_1$ 个被填充的腔的行上．把有 $f_1$ 个被填充的腔的行放在位置 $n+1-f_1$ 上；对列进行重排把被填充的腔推到左边．把有 $f_2$ 个被填充的腔的行放在位置 $n+1-f_1-f_2$ 上；除了第一个 $f_1$，重排其他的列使被填充的腔移到左边；在那行上的前 $f_1+f_2$ 个腔包含被填充的腔．把有 $f_3$ 个被填充的腔放在位置 $n+1-f_1-f_2-f_3$ 上，等等，并继续直到所有被填充的腔在反对角线之上．然后，如果行 $n+1-f_1$ 上包含 $x$ 的腔在列 $j$，交换列 $j$ 和列 $f_1+1$.

由归纳假设，在反对角线之上的部分至多有 $n-1$ 个被填充的腔，可以由除 $x$ 之外的符号补足为阶是 $n$ 的一个拉丁方 $A$．阵列 $B$，如在定理 17.5 中所描述的，包含部分拉丁方的原来被填充的腔，与 $L$ 的不同仅仅是行和列的排列．定理 17.5 说 $B$ 能被补足，因此 $L$ 也能被补足成一个拉丁方．

在此我们也可以断言，如果 $L$ 有一行恰包含一个已填充的腔，或者一列恰包含一个已填充的腔，则 $L$ 也能被补足成一个拉丁方，这是因为 $L$ 的共轭有这样的性质：有一个符号恰出现一次(例如，图 17.4 右方的部分拉丁方的每一行恰包括一个已填充的腔，而且在左方它的共轭具有每个符号恰好出现一次的特性)，而且 $L$ 的共轭能被补足当且仅当 $L$ 能被补足．

于是，我们现在可以断言，没有行或者列恰包含一个已填充的腔．因此，已填充的腔至多被 $m$ 行和 $m$ 列包含，这里 $m := \lfloor n/2 \rfloor$．我们重排行和列，使得所有已填充的腔位于 $m$ 阶的左上方子阵列中．定理 17.4 蕴涵每个 $m\times m$ 拉丁矩形能被补足成阶为 $n+1$ 的拉丁方．填充 $m$ 阶的左上方子阵列中未填充的腔得到一个拉丁矩形就够了．但这是容易的，因为我们有 $n+1$ 个符号可以使用，而且可以以任何顺序用一个在一行或一列中未使用过的符号填充这一行或一列包含的一个腔．■

下面推广拉丁方的思想．假定给定 $n$-集合 $C(i,j)$ 的一个族 $\mathcal{C}$，其中 $i$，$j=1$，2，…，$n$．可以问这样的问题，是否存在大小为 $n\times n$ 的一个矩阵 $A$，分别在其每一行和每一列中，所有的项 $a_{ij}$ 是不同的，且对所有的 $i$ 和 $j$，$a_{ij}\in C(i,j)$．如果所有的 $n$-集合都是$\{1,2,\cdots,n\}$，答案是肯定的，因为拉丁方是一个解．如果$\mathcal{C}$的元素是两两不相交的，这个问题是平凡的．不需要 $n$-集合是相同的而增加的自由度，使问题变得更困难也许出乎意料．事实上，定理 17.1

192

193

的一个类推在这种情况下不成立．在这样的一个矩阵 $A$ 确实存在的猜想被 F. Galvin(1995)证明之前，它以 Dinitz 猜想著称．

我们利用图染色的术语(在第 33 章将详细讨论的一个问题)．设 $G$ 是一个简单图．$G$ 的一个目录分配是函数 $C$，它给 $G$ 的每个顶点 $v$ 分配一个集合 $C(v)$．$G$ 的一个 $C$-染色是定义在顶点集上的函数 $A$，使得 $A(v)\in C(v)$，且如果 $v$ 和 $w$ 在 $G$ 中邻接，$A(v)$和$A(w)$不相同．

设 $f$ 是从 $G$ 的顶点集到整数的一个函数．我们说 $G$ 是 $f$-可染色的，如果对每个 $C$ 有 $G$ 的 $C$-染色存在，$C$ 满足对所有 $v\in G$，$|C(v)|\geqslant f(v)$．如果 $k$ 是一个整数，一个图 $G$ 称为 $k$-目录-可染色的，如果对常数函数 $f(v)=k$，$G$ 是 $f$-可染色的．显然，如果 $G$ 是 $k$-目录-可染色的，那么 $k$ 至少是在第 3 章定义的色数 $\chi(G)$．

简单图 $G$ 的线图 $L=L(G)$是一个简单图，满足 $V(L):=E(G)$，$a$，$b\in E(G)$作为 $L$ 的顶点是邻接的，当且仅当 $a$，$b$ 在 $G$ 中作为边有一个共同的关联顶点．现在考虑 $K_{n,n}$的线图$L_2(n)$(参见第 21 章)．它有 $n^2$ 个顶点$\{i, j\}$，$i$，$j=1, 2, \cdots, n$，这里顶点对被连结当且仅当它们有一个公共的元素．Dinitz 猜想可描述如下：$L_2(n)$是 $n$-目录-可染色的．由 Galvin 证明的定理断言，对二部图 $G$，线图 $L=L(G)$是 $\chi(L)$-目录-可染色的．因为拉丁方存在，$L_2(n)$有色数 $n$，所以 Dinitz 猜想是正确的．

我们证明能得出这个定理的两个命题．

一个有向图 $D$ 的顶点集的子集 $K$ 称为 $D$ 的核，如果 $K$ 中没有两个顶点由一条边相连且对每一个 $v\notin K$，存在一个 $w\in K$，使得在 $D$ 中从 $v$ 到 $w$ 有一条边．

**命题 17.7** *设 $D$ 为其每个诱导子图都有一个核的有向图．对 $D$ 的每个点 $v$，设 $f(v):=1+(v)$的出次，则 $D$ 是 $f$-可染色的．*

194

**证明** 我们对顶点数用归纳法．对顶点数较少的情形易于验证．(注意问题的条件和结论不成立的仅有三个顶点的有向图是有向回路．)

设 $C$ 是 $D$ 的一个目录分配，满足对所有的 $v$，$|C(v)|\geqslant f(v)$．从 $C$ 的一个集合中取一个元素 $x$，考虑使得 $x\in C(v)$的所有顶点 $v$．我们称这些顶点上的诱导子图为 $D_1$．根据假设，$D_1$ 有一个核 $K$．设 $D_2$ 是 $D\setminus K$ 中的顶点上的诱导子图．对一个顶点 $v\notin K$，定义 $C'(v):=C(v)\setminus\{x\}$．由归纳假设 $D_2$ 有一个 $C'$-染色 $A'$．如果我们在 $D$ 上由

$$A(v):=\begin{cases}A'(v) & 若\ v\notin K,\\ x & 若\ v\in K\end{cases}$$

定义 $A$，则显然 $A$ 是 $D$ 的一个 $C$-染色． ■

对下一个命题，我们定义图 $G$ 的一个定向是*正常的*，如果 $G$ 的每一个团是一个可迁竞赛图．

**命题 17.8** *一个二部图 $G$ 的线图 $L=L(G)$的每一个正常定向有一个核．*

**证明** 我们对 $G$ 的边数用归纳法．对边数较少的情形，这个断言易于检验．假设$V(G)=X\cup Y$(以及 $X$ 和 $Y$ 之间的所有边)．我们可以假设 $G$ 的每个顶点有正的次数．设 $D$ 是 $L(G)$的一个正常定向．$L(G)$中的团对应于 $X$ 或 $Y$ 中的顶点．

对每个顶点 $x\in X$，我们考虑 $L(G)$中对应的团并定义 $e(x):=\{x, y(x)\}$为这个团(相对

于 $D$)的收点. 首先，假设对每个 $x\in X$，$L(G)$中的顶点 $e(x)$是由 $y(x)\in Y$ 定义的团中的发点. 那么，显然对 $x\in X$，所有的 $y(x)$是不同的，所以 $K:=\{\{(x, y(x))\}: x\in X\}$是 $L(G)$的一个核.

其次，假设对某个 $x\in X$，$e(x):=\{x, y(x)\}$是对应于 $x$ 的团的收点，但是 $e':=\{x', y(x)\}$是对应于 $y(x)$的团的发点，这里 $x'\neq x$. 从 $G$ 中去掉边$\{x', y(x)\}$. 由归纳假设，得到的线图有一个核 $K$. 我们断言 $K$ 也是 $D$ 的核. 我们必须证明从 $e'$到 $K$ 有一条边，只需 $e(x)\in K$ 即可(因为 $e'$是发点). 然而，如果 $e(x)\notin K$，则存在从 $e(x)$到 $K$ 中的某个元素的一条边，由 $e(x)$的定义，它一定具有类型$\{x'', y(x)\}$. 因为由 $y(x)$定义的竞赛图是可迁的，我们再次证得从 $e'$到 $K$ 有一条边. ■

195

下面证明以下的主要结果.

**定理 17.9**　*如果 $G$ 是一个二部图，则 $L=L(G)$是 $\chi(L)$-可染色的.*

**证明**　设 $G$ 是顶点集 $X\cup Y$ 上的一个二部图. 设 $g$ 是 $L=L(G)$的顶点染颜色 1, 2, …, $\chi(L)$的一个染色. 我们定向 $L$ 以形成一个有向图 $D$：如果 $e_1=\{x_1, y_1\}$和 $e_2=\{x_2, y_2\}$是 $L$ 的相邻顶点且 $g(e_1)<g(e_2)$，则

$$\begin{cases}\text{如果 } x_1=x_2, & \text{边从 } e_1 \text{ 到 } e_2,\\ \text{如果 } y_1=y_2, & \text{边从 } e_2 \text{ 到 } e_1.\end{cases}$$

因为 $L$ 中的每一个团对应一个顶点 $x\in X$ 或 $y\in Y$，所以这一定向是正常的. 由命题 17.8，$D$ 的每个诱导子图有一个核. 显然，对每个顶点 $e\in D$，1+($e$)的出次$<\chi(L)$. 于是，由命题 17.7，证明完成. ■

**问题 17G**　(a)设 $n$ 是偶数. 求$\mathbb{Z}_n$的元素 $x_1, x_2, \cdots, x_n$ 的一个排列，使得差 $x_{i+1}-x_i$($1\leqslant i<n$)全不相同.

(b)证明：如果 $n$ 是奇数，这是不可能的.

(c)考虑(a)中的排列，定义 $a_{ij}:=x_i+x_j$. 证明项为 $a_{ij}$($1\leqslant i, j\leqslant n$)的阵列是具有如下性质的一个拉丁方：$n(n-1)$个相邻的对($a_{ij}$, $a_{i,j+1}$)是不同的. 这样的阵列称为行-完全的. 这个阵列也是列-完全的.

**问题 17H**　描述所有的符号出现在主对角线上的 $n$ 阶对称拉丁方与主对角线上全为 $n+1$ 的 $n+1$ 阶对称拉丁方之间的一个一一对应.

196

**问题 17I**　设 1, 2, …, $n$ 是一个拉丁方的第一行，2, 3, …, $n$, 1 是第二行. 第三行有多少种选择方法?

**问题 17J**　设 1, 2, …, $2n-1$, $2n$ 是一个 $2n$ 阶拉丁方的第一行. 设 2, 1, 4, 3, …, $2n$, $2n-1$ 是第二行.

(i)找出一个公式求第三行有多少种选择方法.

(ii)给出一个积和式，它把以上选择方法数作为值.

## 评注

尽管对拉丁方的研究已超过 200 年，但本章的大多数材料是近期的研究结果. 定理 17.1

是最早的，它属于 M. Hall，Jr.(1945).

定理 17.2 与其后的注记可在 H. J. Ryser(1969)中找到．在这篇论文写作之时，范德瓦尔登猜想仍未解决.

定理 17.3 是新的.

定理 17.4 也属于 H. J. Ryser(1951).

所谓的 Evans 猜想作为一个问题(而不是作为一个猜想)出现在 T. Evans(1960)的一篇论文中．在 B. Smetaniuk 的证明出现之前，有一些部分的结果发表.

本书所介绍的 Dinitz 猜想的 Galvin 证明基于 D. Hoffman 的一些未发表的笔记.

对拉丁方的最为广泛的讨论可参考 J. Dénes and A. D. Keedwell(1991)的书《Latin Squares》.

## 参考文献

J. Dénes and A. D. Keedwell (1991), *Latin squares. New developments in the theory and applications.*, Annals of Discrete Mathematics **46**, North-Holland.

T. Evans (1960), Embedding incomplete Latin squares, *Amer. Math. Monthly* **67**, 958–961.

F. Galvin (1995), The list chromatic index of a bipartite multigraph, *J. Combin. Theory Ser. B* **63**, 153–158.

M. Hall, Jr. (1945), An existence theorem for Latin squares, *Bull. Amer. Math. Soc.* **51**, 387–388.

H. J. Ryser (1951), A combinatorial theorem with an application to Latin rectangles, *Proc. Amer. Math. Soc.* **2**, 550–552. [197]

H. J. Ryser (1969), Permanents and systems of distinct representatives, in: *Combinatorial Mathematics and its Applications*, University of North Carolina Press.

B. Smetaniuk (1981), A new construction on Latin squares I: A proof of the Evans conjecture, *Ars Combinatoria* **11**, 155–172. [198]

# 第 18 章　阿达马矩阵和里德-米勒码

阿达马考虑过如下的问题. 设 $A$ 为一个 $n\times n$ 的实矩阵，它的项的绝对值至多是 1. $A$ 的行列式(按照绝对值)能有多大? 因为 $A$ 的每一列是长度$\leqslant\sqrt{n}$的一个向量，所以行列式不超过 $n^{n/2}$. (行列式的绝对值是在 $n$ 维欧几里得空间中由行向量张成的平行六面体的 $n$ 维体积.)等号能成立吗? 等号成立时每一项一定是 $+1$ 或 $-1$，而且任意两行一定是正交的，即它们的内积为 0. 这引出下面的定义.

*$n$ 阶阿达马矩阵*是项为 $+1$ 或 $-1$ 且使得

$$HH^\top = nI \tag{18.1}$$

的 $n\times n$ 矩阵 $H$. 当然，$H$ 的任意两列也是正交的. 如果交换行或者列，或者把某些行或列乘以 $-1$，正交的性质是不变的. 两个这样的阿达马矩阵称为是等价的. 对一个给定的阿达马矩阵，我们能找到一个等价矩阵，它的第一行和第一列全由 $+1$ 构成. 这样的阿达马矩阵称为规范化阿达马矩阵. 显然，剩余的行(如果有的话)有同样多的 $+1$ 和 $-1$，即如果 $n\neq 1$，则 $n$ 一定是偶数. 一些小例子如下:

$$[1],\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\begin{bmatrix}+ & + & + & +\\ + & + & - & -\\ + & - & + & -\\ + & - & - & +\end{bmatrix},$$

199

在最后一个例子中，我们仅指明项的符号.

**问题 18A**　证明阶为 12 的任意两个阿达马矩阵是等价的.

**定理 18.1**　*如果 $H$ 是阶为 $n$ 的阿达马矩阵，则 $n=1$，$n=2$ 或 $n\equiv 0 \pmod 4$.*

**证明**　设 $n>2$. 规范化 $H$. 我们可以交换 $H$ 的列，使它的前三行变成

$$\begin{array}{cccc}
++\cdots++ & ++\cdots++ & ++\cdots++ & ++\cdots++\\
++\cdots++ & ++\cdots++ & --\cdots-- & --\cdots--\\
\underbrace{++\cdots++}_{a\text{ 列}} & \underbrace{--\cdots--}_{b\text{ 列}} & \underbrace{++\cdots++}_{c\text{ 列}} & \underbrace{--\cdots--}_{d\text{ 列}}
\end{array}$$

我们有 $a+b+c+d=n$，由这些行构成的三个内积产生 $a+b-c-d=0$，$a-b+c-d=0$，$a-b-c+d=0$. 如果把这些等式相加，得到 $n=4a$，这就证明了定理. (类似地，可以看到 $4b=4c=4d=n$.) ■

组合设计领域中的一个著名猜想说，对每一个 $n\equiv 0 \pmod 4$ 存在阶为 $n$ 的一个阿达马矩阵. 我们现在离这个猜想的证明仍然非常遥远. 目前，可能存在但仍然没有例证的阿达马矩阵的最小阶为 428. 有许多构造阿达马矩阵的方法，我们将讨论其中的几个. 首先我们定义与阿达马矩阵非常类似的矩阵的第二个类.

*$n$ 阶会议矩阵 $C$* 是 0 在主对角线上，$+1$ 和 $-1$ 在所有其他的位置，且有性质

$$CC^\top = (n-1)I \tag{18.2}$$

的 $n\times n$ 矩阵．会议矩阵的名字源于对会议电话线路的一个应用．V. Belevitch(1950)研究了所谓由理想的变压器构成的理想无耗散网络，设想的线路打算用于建立一个会议电话网络．该理论导致这样一个网络存在的必要条件，即 $n$ 阶会议矩阵的存在性，这里 $n$ 是网络终端的数目．这就解释了会议矩阵的名字．

**问题 18B** 设 $C$ 为一个阶 $n\neq 1$ 的会议矩阵．证明 $n$ 是偶数．通过交换行和列以及特定的行和列乘以 $-1$ 证明，我们能找到一个等价的会议矩阵，如果 $n\equiv 2 \pmod 4$，它是对称的；如果 $n\equiv 0 \pmod 4$，它是反对称的． [200]

**定理 18.2** 如果 $C$ 是一个反对称的会议矩阵，则 $I+C$ 是一个阿达马矩阵．

**证明** $(I+C)(I+C)^{\top}=I+C+C^{\top}+CC^{\top}=I+(n-1)I=nI.$ ■

**定理 18.3** 如果 $C$ 是一个 $n$ 阶对称矩阵，则

$$H=\begin{bmatrix} I+C & -I+C \\ -I+C & -I-C \end{bmatrix}$$

是一个 $2n$ 阶阿达马矩阵．

**证明** 计算 $HH^{\top}$就可以得出结果． ■

有些组合结构的最常见的构造方法之一是所谓的递归方法，其中所需类型的大的对象通过应用某个程序到同一类型的两个或多个较小的对象而得．在下个定理中，我们证明构造阿达马矩阵的这样一个方法．

设 $A$ 是项为 $a_{ij}$ 的一个 $m\times n$ 阶矩阵，$B$ 为另一个矩阵．矩阵

$$\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

由 $mn$ 个大小为 $B$ 的块构成，称之为矩阵 $A$ 和 $B$ 的克罗内克(Kronecker)积 $A\otimes B$.

**定理 18.4** 如果 $H_m$ 和 $H_n$ 分别是阶为 $m$ 和 $n$ 的阿达马矩阵，则 $H_m\otimes H_n$ 是阶为 $mn$ 的阿达马矩阵．

**证明** 由直接的计算看出

$$(A\otimes B)(C\otimes D)=(AC)\otimes(BD),$$ [201]

而且

$$(A\otimes B)^{\top}=A^{\top}\otimes B^{\top}.$$

我们取 $A=C=H_m$ 且 $B=D=H_n$．结果由阿达马矩阵的定义和 $I_m\otimes I_n=I_{mn}$ 这一事实得到． ■

把这个定理重复用于 $\boldsymbol{H}_2:=\begin{bmatrix} + & + \\ + & - \end{bmatrix}$，可以得到阿达马矩阵的一个序列，用 $\boldsymbol{H}_n$ 表示，这里 $n=2^m$，$m=1, 2, \cdots$.

现在我们开始一个直接构造会议矩阵的方法，这些矩阵可以用于定理 18.2 和定理 18.3 以构造阿达马矩阵．在下面，$q$ 是一个奇素数的幂．在域 $\mathbb{F}_q$ 上，用

$$\chi(x):=\begin{cases}0 & \text{如果 } x=0,\\ 1 & \text{如果 } x \text{ 是一个非零的平方},\\ -1 & \text{如果 } x \text{ 不是一个平方}\end{cases}$$

定义一个函数 $\chi$(称为特征). 对$\mathbb{F}_q$ 中的任意 $x$ 和 $y$，我们有 $\chi(x)\chi(y)=\chi(xy)$，而且由于非零的平方数和非平方数一样多，我们有

$$\sum_{x\in\mathbb{F}_q}\chi(x)=0. \tag{18.3}$$

现在设 $0\neq c\in\mathbb{F}_q$，那么 18.3 蕴涵

$$\sum_{b\in\mathbb{F}_q}\chi(b)\chi(b+c)=-1. \tag{18.4}$$

这可由忽略等于 0 的项 $b=0$，然后把 $\chi(b+c)$写或 $\chi(b)\chi(1+cb^{-1})$看出(注意 $\chi(b)^2=1$，如果 $b\neq0$). 如果 $b$ 取遍这个域的所有非零元，那么 $1+cb^{-1}$取除 1 之外的所有值.

对$\mathbb{F}_q$的元素编号：$0=a_0$，$a_1$，…，$a_{q-1}$. 由

202

$$q_{ij}:=\chi(a_i-a_j),\quad 0\leqslant i,j<q$$

定义一个 $q\times q$ 矩阵 $Q$. 注意到，如果 $q\equiv1(\bmod 4)$，$Q$ 是对称的；如果 $q\equiv3(\bmod 4)$，$Q$ 是反对称的. 作为 $\chi$ 的基本性质和(18.4)的一个直接结论，我们发现 $QQ^{\top}=qI-J$ 且 $QJ=JQ=O$. 大小为$(q+1)\times(q+1)$的矩阵 $C$ 由

$$C:=\begin{bmatrix}0 & 1\ \ 1 & \cdots & 1\\ \pm1 & & & \\ \vdots & & Q & \\ \pm1 & & & \end{bmatrix} \tag{18.5}$$

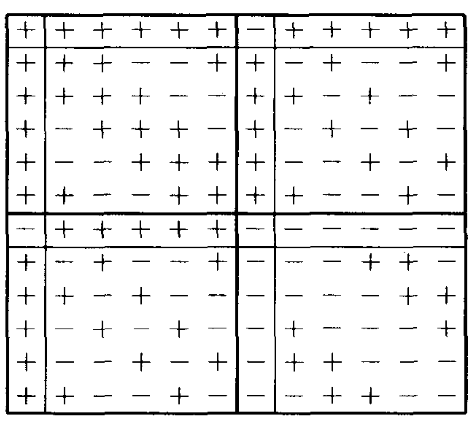
定义，这里项$\pm1$ 的符号如下选择：$C$ 是对称的或反对称的. 由 $Q$ 的性质，得出 $C$ 是阶为 $q+1$ 的会议矩阵. 这种构造方法属于 Paley(1933)且这种类型的会议矩阵通常称为 Paley 矩阵. 对 $q$ 是一个素数的特殊情况，矩阵 $Q$ 是循环的. 我们把这种构造方法总结为一个定理.

**定理 18.5**　*设 $q$ 是一个奇素数的幂，如果 $q\equiv3(\bmod 4)$，存在阶为 $q+1$ 的阿达马矩阵；如果 $q\equiv1(\bmod 4)$，存在阶为 $2(q+1)$的阿达马矩阵.*

图 18.1 和 18.2 分别图示了从阶为 11+1 和 5+1 的 Paley 矩阵构造阶为 12 的阿达马矩阵.

| + | + | + | + | + | + | + | + | + | + | + | + |
|---|---|---|---|---|---|---|---|---|---|---|---|
| − | + | + | − | + | + | + | − | − | − | + | − |
| − | − | + | + | − | + | + | + | − | − | − | + |
| − | + | − | + | + | − | + | + | + | − | − | − |
| − | − | + | − | + | + | − | + | + | + | − | − |
| − | − | − | + | − | + | + | − | + | + | + | − |
| − | − | − | − | + | − | + | + | − | + | + | + |
| − | + | − | − | − | + | − | + | + | − | + | + |
| − | + | + | − | − | − | + | − | + | + | − | + |
| − | + | + | + | − | − | − | + | − | + | + | − |
| − | − | + | + | + | − | − | − | + | − | + | + |
| − | + | − | + | + | + | − | − | − | + | − | + |

图　18.1



| + | + | + | + | + | + | − | + | + | + | + | + |
|---|---|---|---|---|---|---|---|---|---|---|---|
| + | + | + | − | − | + | + | − | + | − | − | + |
| + | + | + | + | − | − | + | + | − | + | − | − |
| + | − | + | + | + | − | + | − | + | − | + | − |
| + | − | − | + | + | + | + | − | − | + | − | + |
| + | + | − | − | + | + | + | + | − | − | + | − |
| − | + | + | + | + | + | − | − | − | − | − | − |
| + | − | + | − | − | + | − | − | − | + | + | − |
| + | + | − | + | − | − | − | − | − | − | + | + |
| + | − | + | − | + | − | − | + | − | − | − | + |
| + | − | − | + | − | + | − | + | + | − | − | − |
| + | + | − | − | + | − | − | − | + | + | − | − |

图　18.2

**问题 18C** 证明：如果 $n\equiv 0(\bmod 4)$，$n\leqslant 100$，除了可能的 $n=92$ 外，存在一个阶为 $n$ 的阿达马矩阵.

在 Paley 的结果与由 L. D. Baumert. S. W. Golomb 和 M. Hall 发现 92 阶阿达马矩阵之间有 30 年的时间. 他们所用的方法在 1944 年被 Williamson 发展，但找到实实在在的矩阵，计算机搜索是必不可少的. Williamson 的方法基于如下观察：设 $A_i(1\leqslant i\leqslant 4)$是 $n$ 阶对称矩阵，$n$ 为奇数，再假设它们彼此交换，考虑由

$$\begin{bmatrix} A_1 & A_2 & A_3 & A_4 \\ -A_2 & A_1 & -A_4 & A_3 \\ -A_3 & A_4 & A_1 & -A_2 \\ -A_4 & -A_3 & A_2 & A_1 \end{bmatrix} \tag{18.6}$$

定义的矩阵 $H$. 那么，我们有

203~204

$$HH^{\top} = I_4 \otimes (A_1^2 + A_2^2 + A_3^2 + A_4^2). \tag{18.7}$$

为了以这种方式构造一个阿达马矩阵，我们必须找到满足上述条件的矩阵 $A_i$，它们的项为 $\pm 1$，此外还满足

$$A_1^2 + A_2^2 + A_3^2 + A_4^2 = 4nI_n. \tag{18.8}$$

设 $U$ 是对应于置换$(12\cdots n)$的 $n$ 阶置换矩阵，即 $u_{ij}=1$ 当且仅当 $j-i\equiv 1(\bmod n)$. 那么 $U^n=I$ 且任意的循环矩阵是 $U$ 的幂的线性组合. 如果假设 $A_i$ 具有形式 $A_i=\sum_{j=0}^{n-1} a_{ij}U^j$，$a_{i0}=1$ 且$a_{ij}=a_{i,n-j}$，则这些矩阵确实是交换的并且是对称的. 从现在起，我们还假定所有的 $a_{ij}$ 是$\pm 1$ 且满足(18.8). 取 $n=3$，$A_1=J$，且 $A_i=J-2I$，$i=2$，3，4，可以找到按这种方法构造阿达马矩阵的一个简单例子. 我们找到阶为 12 的一个阿达马矩阵，见图 18.3.

$$\left[\begin{array}{ccc|ccc|ccc|ccc}
+ & + & + & - & + & + & - & + & + & - & + & + \\
+ & + & + & + & - & + & + & - & + & + & - & + \\
+ & + & + & + & + & - & + & + & - & + & + & - \\ \hline
+ & - & - & + & + & + & + & - & - & - & + & + \\
- & + & - & + & + & + & - & + & - & + & - & + \\
- & - & + & + & + & + & - & - & + & + & + & - \\ \hline
+ & - & - & - & + & + & + & + & + & + & - & - \\
- & + & - & + & - & + & + & + & + & - & + & - \\
- & - & + & + & + & - & + & + & + & - & - & + \\ \hline
+ & - & - & + & - & - & - & + & + & + & + & + \\
- & + & - & - & + & - & + & - & + & + & + & + \\
- & - & + & - & - & + & + & + & - & + & + & +
\end{array}\right]$$

图 18.3

**例 18.1** 注意，在我们的构造中蕴涵 $A_i$ 有常数的行和 $a_i$(奇数)，且由(18.8)有 $a_1^2+\cdots+a_4^2=4n$. 如果希望用这种方法寻找阶为 20 的一个阿达马矩阵，首先把 20 写成四个奇数平方的和：$20=9+9+1+1$. 由此可以看出 $A_i$ 中的两个一定是 $2I-J$，之后不难看出其他两个矩阵的第一行分别是$+-++-$，$++--+$.

205

为了再进一步分析这种情况，我们引入矩阵 $W_i$ 和 $P_i$ 如下：

$$2W_i := (A_1 + \cdots + A_4) - 2A_i, \tag{18.9}$$

$$A_i = 2P_i - J. \tag{18.10}$$

对系数 $a_{ij}$ 的约定蕴涵，如果 $p_i$ 由 $p_iJ := P_iJ$ 定义，则 $p_i$ 是一个奇整数. 此外，(18.8)和(18.9)蕴涵

$$W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4nI. \tag{18.11}$$

在(18.8)中代入(18.10)，可以发现

$$\sum_{i=1}^{4} P_i^2 = \Big(\sum_{i=1}^{4} p_i - n\Big)J + nI. \tag{18.12}$$

假设项 $U^k(k\neq 0)$在矩阵 $P_i$ 的 $\alpha$ 个中出现. 考虑等式(18.12)mod 2，在等式的左边我们发现 $U^{2k}$的系数为$\alpha$，且在右边 $U^{2k}$的系数是 1. 于是 $\alpha$ 为奇数，这蕴涵着 $U^k$ 恰好在矩阵 $W_i$(带系数±2)的一个中出现. 从例 18.1 和(18.9)可以看到矩阵 $W_i$ 的常数行和 $w_i$ 满足 $w_1^2+\cdots+w_4^2=4n$. 这些事实减少了也满足(18.11)的可能矩阵 $W_i$ 的数目，使计算机寻找这些矩阵是可行的. $A_i$ 随之可由(18.9)而得下面列出阶为 23 的四个矩阵的第一行，它们产生了第一个 92 阶的阿达马矩阵.

$A_1$:　++−−−+−−−+−++−+−−−+−−−+

$A_2$:　+−++−++−−++++++−−++−++−

$A_3$:　+++−−−++−+−++−+−++−−−++

$A_4$:　+++−+++−+−−−−−−−+−+++−++

**问题 18D**　利用 Williamson 方法构造阶为 28 的一个阿达马矩阵.

206　下面考察关于阿达马矩阵的一个不同问题. 如果一个 $n$ 阶阿达马矩阵被规范化，显然它的+1 项比−1 项恰好多 $n$. 定义一个阿达马矩阵的超出量是它的所有项的和，然后定义 $\sigma(n)$为所有 $n$ 阶阿达马矩阵的超出量的最大值. 下面的界属于 Best(1977)，它证明 $\sigma(n)$如同 $n^{3/2}$那样增长.

**定理 18.6**　$n^2 2^{-n}\binom{n}{\frac{1}{2}n}\leqslant\sigma(n)\leqslant n\sqrt{n}$.

**证明**　(a)设 $H$ 为一个 $n$ 阶阿达马矩阵，$s_k$ 为 $H$ 第 $k$ 列的和. 设 $\boldsymbol{c}_i$ 为 $H$ 的第 $i$ 行，其中 $1\leqslant i\leqslant n$. 我们用两种方式计算 $\sum_{1\leqslant i,j\leqslant n}\langle \boldsymbol{c}_i, \boldsymbol{c}_j\rangle$. 由阿达马矩阵的定义，这个和是 $n^2$. 另一方面

$$\sum_{1\leqslant i,j\leqslant n}\sum_{k=1}^{n} c_{ik}c_{jk} = \sum_{k=1}^{n} s_k^2.$$

由这个等式和柯西-施瓦茨不等式，我们发现

$$\sum_{k=1}^{n} s_k \leqslant \Big(n\sum_{k=1}^{n} s_k^2\Big)^{1/2} = n\sqrt{n},$$

于是 $\sigma(n)\leqslant n\sqrt{n}$.

(b)设 $\boldsymbol{x}$ 为$\{+1, -1\}^n$ 中的任意一个向量，我们用 $x_j$ 乘 $H$ 的列 $j$，$1\leqslant j\leqslant n$. 随后，用−1 乘那些−1 项比+1 项多的行. 称得到的矩阵为 $H_x$ 并定义 $\sigma(H_x):=\sum_{i=1}^{n}|\langle \boldsymbol{x}, \boldsymbol{c}_i\rangle|$. 显然 $\sigma(n)$至少等于 $\sigma(H_x)$的平均值. 于是我们得到

$$\sigma(n)\geqslant 2^{-n}\sum_{x\in\{+1,-1\}^n}\sigma(H_x) = 2^{-n}\sum_{x}\sum_{i=1}^{n}|\langle \boldsymbol{x},\boldsymbol{c}_i\rangle|$$

$$= 2^{-n}\sum_{i=1}^{n}\sum_{d=0}^{n}\sum_{x,d(x,c_i)=d}|n-2d|$$

$$= 2^{-n} n \sum_{d=0}^{n} |n-2d| \binom{n}{d} = n^2 2^{-n} \binom{n}{\frac{1}{2}n}.$$ ■ [207]

**推论** $2^{-1/2} n^{3/2} \leqslant \sigma(n) \leqslant n^{3/2}$.

**证明** 由斯特林公式，定理18.6中不等式的左边渐近地等于 $2^{1/2}\pi^{-1/2}n^{3/2}$. 为了得到对所有的 $n$ 成立的不等式，我们必须用 $2^{-1/2}$ 代替常数 $2^{1/2}\pi^{-1/2}$. ■

**例 18.2** 考虑 $4\times4$ 的一个方阵，它被分成16个腔，从1～16对它们编号. 行为 $a_i(1\leqslant i\leqslant16)$ 的一个矩阵 $A$ 如下定义：如果 $j$ 与 $i$ 在方阵中出现在同一行或同一列，但是 $j\neq i$，$a_{ij}=-1$；否则，$a_{ij}=1$. 对 $A$ 的任意两行，存在两个位置，其项都是 $-1$. 因此 $A$ 是超出量为64的16阶阿达马矩阵，即对于这个矩阵，在定理18.6中上界取等号.

这个阿达马矩阵也可构造如下. 定义 $H:=J-2I$ 是一个有最大超出量的4阶阿达马矩阵，超出量为8. $H$ 的每一行的 $+1$ 项的数目相同，即是3. 矩阵 $H\otimes H$ 是阶为16的阿达马矩阵，每一行有10个 $+1$ 项，该矩阵有最大的超出量64. 如果我们取这个矩阵与 $H$ 的克罗内克积，我们又找到一个行和为常数且有最大超出量的阿达马矩阵，等等. 一般来说，一个阶为 $4u^2$ 的阿达马矩阵，其所有的列和等于 $2u$，且因此该矩阵有最大的超出量，这样的矩阵称为*正则阿达马矩阵*. 已知这种矩阵的其他一些构造方法.

在阿达马矩阵的应用中，非常有趣且非常成功的是它们被用作*纠错码*. 许多读者可能看过诸如水手号、旅行者号[⊖]之类的人造卫星拍摄的火星、土星和其他行星的精美照片. 为了把这样一张照片传送到地球上，首先把照片分得非常小(*像素*)，对每个这样的正方形的黑度进行测量并表示出来，比如说，用0～63的一个等级，这些数用二进制表示，即每个像素产生六个0和1(比特)的一个串. 比特被转送到地球上的接收站(位于加州理工学院的喷气推进实验室). 由于一些*噪声*源，其中之一是放大器的热噪声，偶尔会发生一个作为0传送的信号被作为1接收，1作为0被接收. 如果每个六元组对应的一个像素被如此传送，那么由接收机所犯的错误会使图像质量很差. 因为只有有限的时间传送照片，而且来自太阳能电池板的能量有多少是已知的，所以我们知道要产生被送到接收机的信号的每一比特的平均能量. 由此可以计算(每比特的)错误概率 $p$. [208]

假设对一张有用的照片，每个六元组出错的概率 $P_E$ 至多为 $10^{-4}$. 为了通过简单的比特传送达到这个概率，我们需要 $p\approx10^{-4}/6$，因为 $P_E=1-(1-p)^6\approx10^{-4}$. 首先假设可以得到所需的能量，通过如下的做法尝试提高照片的质量：代替发送一个比特，比如说0，我们发送五个0，并且接收机把接收到的五元组译成发生次数最多的那个比特. 我们正在用一种码，它是有两个长度为5的字的*重复码*，两个字为00000和11111. 数值1/5称为这个码的*信息率*. 能量的限制允许我们计算每个信道比特有多少能量可以利用. 此后，可以计算新的(每个信道比特的)错误率 $p'$. 当然 $p'>p$，且在我们的例子中，事实上，$p'=0.035$(差不多是不用编码的2000倍). 仅在纠错足以弥补每比特能量的损失时编码才有意义.

传送的一个六元组被正确地接收的概率现在变成

⊖ 这是美国发射的宇宙飞船. ——译者注

$$[(1-p')^5+5p'(1-p')^4+10(p')^2(1-p')^3]^6,$$

即≈0.997，换言之，我们已彻底地损坏了照片！

现在让我们来看看在 1969 年水手号的探险中实际上是怎么做的. 64 个可能的信息串(对应像素可能的黑度)被映射到矩阵 $\boldsymbol{H}_{32}$ 和 $-\boldsymbol{H}_{32}$ 的行. 因为现在我们有表示长度为 6 的信息字的长度为 32 的码字，所以信息率是 6/32，差不多与重复码的信息率相同. 注意这些码字中的任意两个或者在所有的 32 个位置上不同，或者恰好在其中的 16 个位置上不同. 于是，如果接收到的一个字至多包含 7 个错误，则它比其余 63 个字中的任何一个更接近正确的字.（我们已把符号 0 和 1 换成±1.）我们说这个码是一个 7-纠错码. 现在，新的错误概率是 $p'\approx0.036$(仍较大)，一个接收到的字被不正确地译码的概率是

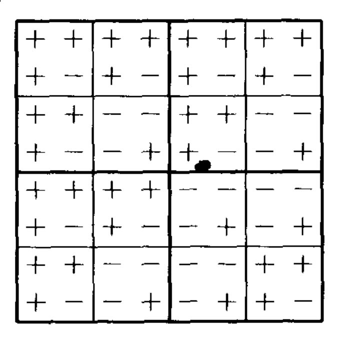
209

$$\sum_{i=8}^{32}\binom{32}{i}(p')^i(1-p')^{32-i},$$

这差不多等于 $1.4\cdot10^{-5}$，在大小的阶上比 $P_E$ 好.

在实际中，不应用这个码就没有足够的能量来传递质量较高的图片，这一问题已得以解决.

我们所看到的(低比率)码的序列的一个例子，以一阶里德-米勒(Reed-Muller)码而知名. 再次考虑阿达马矩阵 $\boldsymbol{H}_n$ 的构造，这里 $n=2^m$. 图 18.4 中给出了 $\boldsymbol{H}_8$.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| + | + | + | + | + | + | + | + |
| + | − | + | − | + | − | + | − |
| + | + | − | − | + | + | − | − |
| + | − | − | + | + | − | − | + |
| + | + | + | + | − | − | − | − |
| + | − | + | − | − | + | − | + |
| + | + | − | − | − | − | + | + |
| + | − | − | + | − | + | + | − |

图 18.4

在矩阵 $\boldsymbol{H}_n$ 中，用 0 代替每个+1 且用 1 代替每个−1. 从 0 到 $n-1=2^m-1$ 对行编号. 当我们从 $m$ 到 $m+1$，即把矩阵的阶加倍时，在克罗内克积构造中会发生什么？新的行(现在视为 $\mathbb{F}_2^{2n}$ 中的向量)对 $0\leqslant i<n$ 具有形式 $(\boldsymbol{c}_i,\boldsymbol{c}_i)$，且对 $n\leqslant i<2n$ 具有形式 $(\boldsymbol{c}_i,\boldsymbol{c}_i+\boldsymbol{1})$，这里 $\boldsymbol{1}$ 表示全是 1 的向量.

210

**定理 18.7** *设 $R'(1,m)$ 表示如上所述的从 $\boldsymbol{H}_n$ 得到的 $\mathbb{F}_2^n$ 中行向量的集合，则 $R'(1,m)$ 是 $\mathbb{F}_2^n$ 的一个 $m$ 维子空间.*

**证明** 对 $m=1$，断言是平凡的. 下面用归纳法证明. 设 $\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_m$ 是 $R'(1,m)$ 的一组基. 上面所做的观察表明 $R'(1,m+1)$ 由向量 $(\boldsymbol{v}_i,\boldsymbol{v}_i)$ 和向量 $(\boldsymbol{0},\boldsymbol{1})$ 的所有线性组合构成，这就完成了证明. ■

现在我们定义长度 $n=2^m$ 且维数为 $m+1$ 的一阶里德-米勒码 $R(1,m)$，它是由空间 $R'(1,m)$ 和长度为 $n$ 的全幺向量张成的 $\mathbb{F}_2^n$ 的子空间. 按这种术语，1969 年水手号用的码是 $R(1,5)$. 从阿达马矩阵的性质，马上看到 $R(1,m)$ 中任意两个码字至少在 $\frac{1}{2}n$ 个位置上不同. 我们说该码有*最小距离* $d=2^{m-1}$. 于是，该码可纠正直到 $2^{m-2}-1$ 个错误.

我们能给出码字一个很好的几何解释. 通过把一个向量看成数的二进制表示来给空间 $\mathbb{F}_n^m$ 的点编号. 例如，(0，1，1，0，1)可看成 $\mathbb{F}_2^5$ 中的点 $P_{22}$. 设这些表示是一个 $m\times n$ 矩阵的列. 再设 $\boldsymbol{v}_i$ 是这个矩阵的第 $i$ 行，$1\leqslant i\leqslant m$. 那么，从图 18.4 和上面的观察可以看到诸向量 $\boldsymbol{v}_i$ 是 $R'(1,m)$ 的自然基. 基向量 $\boldsymbol{v}_i$ 是超平面 $\{(x_1,x_2,\cdots,x_m)\in\mathbb{F}_2^m:x_i=1\}$ 的特征函数. 通过取线性组合，我们看到 $R(1,m)$ 的码字恰好是向量空间 $R'(1,m)$ 中的仿射超平面的所有特征函数、该空间自身(对 $\boldsymbol{1}$)的特征函数，以及空集(对 $\boldsymbol{0}$)的特征函数. 任意两个超平面或者平行，

或者在维数为 $m-2$ 的一个仿射子空间中相交，与阿达马矩阵的两行恰在一半的位置上有相同项这一事实相符.

正如 $R(1, m)$的定义所建议的，高阶里德-米勒码也在纠错码理论中定义. 它们也有一个几何解释，这里我们不打算涉及(但参见例 26.4).

211

**问题 18E** 对 $n=2^m$ 和 $1\leqslant i\leqslant m$，由

$$M_n^{(i)} := I_{2^{m-i}} \otimes \boldsymbol{H}_2 \otimes I_{2^{i-1}}$$

定义矩阵 $M_n^{(i)}$. 证明

$$\boldsymbol{H}_n = M_n^{(1)} M_n^{(2)} \cdots M_n^{(m)}.$$

接收到的一个字 $\boldsymbol{x}$ 由计算 $\boldsymbol{x}\boldsymbol{H}_n^{\mathrm{T}}$ 译码. 如果没有太多的错误，则这个积的所有项除了一项的绝对值接近 $n$ 之外都差不多为 0. 乘以 $\pm1$ 的一个乘法称为一次运算. 比较当用 $\boldsymbol{H}_n$ 以及用 $\boldsymbol{H}_n$ 的表示作为矩阵 $M_n^{(i)}$ 的乘积时，译码必须做的运算的数目. (这是以快速傅里叶变换著称的理论中的一个例子.)

**问题 18F** 设$\boldsymbol{v}_i(0\leqslant i\leqslant m)$是上面给定的 $R(1, m)$的一组基，这里$\boldsymbol{v}_0=\boldsymbol{1}$. 考虑由所有向量

$$\boldsymbol{v}_i \cdot \boldsymbol{v}_j := (v_{i0}v_{j0}, \cdots, v_{i,n-1}v_{j,n-1})$$

张成的$\mathbb{F}_2^n$的子空间 $R(2, m)$，这里 $n=2^m$. 这个空间的维数是多少? 证明 $R(2, m)$的任意两个向量至少在$\frac{1}{4}n$ 个位置不同.

**问题 18G** 假设 $M$ 是一个 $m\times n$ 的(0, 1)-矩阵，使得任意两个不同行之间的汉明距离至少是 $d$. (如果 $M$ 是这样得到的结果：把阿达马矩阵 $H$ 放在 $-H$ 的顶上，并把符号换为 0 和 1，我们就有 $m=2n$ 且 $d=n/2$ 的一个例子.)

(1)以两种方式对有序三元组$(i, j, k)$的数目计数，使得 $i$ 和 $j$ 是不同的行(的指标)，且 $k$ 是一个列的指标，这里 $M(i, k)\neq M(j, k)$——一种方式产生涉及 $d$ 的一个不等式，另一种方式涉及 $M$ 的列和. 证明：如果 $2d>n$，则

$$m \leqslant \frac{2d}{2d-n}.$$

(在编码理论中这个不等式以 Plotkin 界著称.)何种条件保证相等性?

212

(2)假设 $d=n/2$. 证明 $m\leqslant 2n$，再证明相等性蕴涵存在一个 $n$ 阶阿达马矩阵.

**问题 18H** 设 $H$ 为一个 $m$ 阶阿达马矩阵且 $C$ 是一个 $n$ 阶对称会议矩阵. 设 $P$ 为形如 $\begin{bmatrix} O & -I \\ I & O \end{bmatrix}$的大小为 $m$ 的矩阵，这里子矩阵的大小为 $m/2$. 证明$(H\otimes C)+(PH\otimes I)$是一个大小为 $mn$ 的阿达马矩阵.

**问题 18I** 设 $q$ 是一个素数幂，$q\equiv1 \pmod 4$. 设 $C$ 为(18.5)的矩阵. 如同在问题 18H 中那样选择 $H$ 和 $P$. 证明

$$(H \otimes C \otimes Q) + (PH \otimes C \otimes I_q) + (H \otimes I_{q+1} \otimes J_q)$$

是一个大小为 $mq(q+1)$的阿达马矩阵.

## 评注

阿达马(J. Hadamard，1865—1963)是 19 世纪和 20 世纪之交的一个重要数学家. 他最重

要的工作是在解析函数论和数学物理方面. 他最著名的工作是与 C. J. De La Vallée -Poussin 共同完成的所谓素数定理的证明.

R. E. A. C. Paley(1907—1933)在 26 岁滑雪时死于雪崩. 在他短暂的一生中他写了 26 篇高质量的论文(大多是关于傅里叶理论的).

H. J. Ryser 的一个长期未解决的猜想断言，阶数 $n>4$ 的阿达马矩阵不可能是一个循环矩阵.

J. S. Wallis(aka J. Seberry)(1976)证明，对任意整数 $s$，只要 $t>2\log_2(s-3)$就存在 $2^t s$ 阶阿达马矩阵. 然而，仍不知道阿达马矩阵的阶的集合是否有"正的密度".

关于纠错码的更多论述，见第 20 章.

现在称为里德-米勒码的码(令人惊奇地)却是由 D. E. Muller(1954)和 I. S. Reed(1954)首先讨论的.

213 有关水手号航行的编码和译码的详细论述，见 E. C. Posner(1968).

## 参考文献


L. D. Baumert, S. W. Golomb, and M. Hall, Jr. (1962), Discovery of a Hadamard matrix of order 92, *Bull. Amer. Math. Soc.* **68**, 237–238.

V. Belevitch (1950), Theory of $2n$-terminal networks with applications to conference telephony, *Electrical Communication* **27**, 231–244.

M. R. Best (1977), The excess of a Hadamard matrix, *Proc. Kon. Ned. Akad. v. Wetensch.* **80**, 357–361.

D. E. Muller (1954), Application of Boolean algebra to switching circuit design and to error detection, *IEEE Trans. Computers* **3**, 6–12.

R. E. A. C. Paley (1933), On orthogonal matrices, *J. Math. Phys.* **12**, 311–320.

E. C. Posner (1968), Combinatorial structures in planetary reconnaissance, in: *Error Correcting Codes* (H. B. Mann, ed.), J. Wiley and Sons.

I. S. Reed (1954), A class of multiple-error-correcting codes and the decoding scheme, *IEEE Trans. Information Theory* **4**, 38–49.

J. S. Wallis (1976), On the existence of Hadamard matrices, *J. Combinatorial Theory* (A) **21**, 188–195.

J. Williamson (1944), Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11**, 65–81.


214

# 第19章　设　　计

本章介绍组合论中的一个广泛且重要的领域，通常称为设计理论．在这一理论中最普遍的研究对象是所谓的关联结构．这是一个三元组 $\boldsymbol{S}=(\mathcal{P}, \mathcal{B}, \boldsymbol{I})$，其中

(1)$\mathcal{P}$是一个集合，其中的元素称为点．

(2)$\mathcal{B}$是一个集合，其中的元素称为区组．

(3)$\boldsymbol{I}$ 是$\mathcal{P}$和$\mathcal{B}$之间的一个关联关系(即 $\boldsymbol{I}\subseteq\mathcal{P}\times\mathcal{B}$)．$\boldsymbol{I}$ 中的元素称为旗标．

如果$(p, B)\in\boldsymbol{I}$，那么我们说点 $p$ 和区组 $B$ 是关联的．我们允许两个不同的区组 $B_1$ 和 $B_2$ 与$\mathcal{P}$的点的同一个子集关联．在这种情形就称为"重复区组"．如果这种情形不发生，则这一设计称为简单设计，而且可以把区组作为$\mathcal{P}$的子集．事实上，从现在起我们经常要做的，就是仔细区分可能是$\mathcal{P}$的同一子集的不同区组．这允许我们用 $p\in B$ 代替记号$(p, B)\in\boldsymbol{I}$，并且经常说点 $p$"在区组 $B$ 中"而不说 $p$ 与 $B$ 关联．

习惯上，用 $v$ 表示$\mathcal{P}$的基数，用 $b$ 表示$\mathcal{B}$的基数．于是关联结构是 $v$ 个点的一个集合和这个点集合的 $b$ 个未必相异的子集的一个集合．在每个区组中取其补得到的结构自然称为该结构的补．(这意味着在$\mathcal{P}\times\mathcal{B}$中用 $\boldsymbol{I}$ 的补代替 $\boldsymbol{I}$．)

为了得到一个有趣的理论，我们必须在结构 $\boldsymbol{S}$ 上附加一些正则条件．作为第一个例子，我们提及的关联结构有能引起混淆的名字"线性空间"．这里区组通常称为线，正则条件是每条线包含(即关联于)至少两个点，而且任意两个点正好在一条线上．下面的例 19.6 展示了一个简单但重要的线性空间．下面的定理属于 De Bruijn and Erdös(1948)，其简洁的证明属于 Conway．



**定理 19.1**　对一个线性空间，我们有 $b=1$ 或 $b\geqslant v$，且等式蕴涵任意两条线恰有一点与这两条线关联．

**证明**　对 $x\in\mathcal{P}$，用 $r_x$ 表示与 $x$ 关联的线的数目，类似地，对 $B\in\mathcal{B}$，设 $k_B$ 是在 $B$ 上的点的数目．设线多于一条．如果 $x\notin L$，那么 $r_x\geqslant k_L$，因为有 $k_L$ 条线"连结"$x$ 和 $L$ 上的点．假设 $b\leqslant v$，则 $b(v-k_L)\geqslant v(b-r_x)$，且因此

$$1=\sum_{x\in\mathcal{P}}\sum_{x\notin L}\frac{1}{v(b-r_x)}\geqslant\sum_{L\in\mathcal{B}}\sum_{x\notin L}\frac{1}{b(v-k_L)}=1,$$

这蕴涵在所有的不等式中，相等性必须成立．因此，如果 $x\notin L$，$v=b$ 且 $r_x=k_L$．■

定理 19.1 中相等性的一个平凡例子是所谓的拟束，它是这样一个结构：一条线包含除一点之外的所有点，而且包含那个点的所有对作为规模为 2 的线．更有趣的例子是射影平面，我们将在本章的后面定义．所有的可能性就是这些．参见问题 23C．作为一个练习，读者可以对线性空间证明这一事实．

在本章的其余部分，我们主要讨论高度规则的关联结构，称之为"$t$-设计"．设 $v$，$k$，$t$ 和 $\lambda$ 是 $v\geqslant k\geqslant t\geqslant 0$ 且 $\lambda\geqslant 1$ 的整数．在 $v$ 个点上，区组规模为 $k$、指标为 $\lambda$ 的一个 $t$-设计是关联结构 $\mathcal{D}=(\mathcal{P}, \mathcal{B}, \boldsymbol{I})$，满足：

(i) $|\mathcal{P}|=v$.

(ii)对所有的 $B\in\mathcal{B}$，$|\mathcal{B}|=k$.

(iii)对 $t$ 个点的任意集合 $T$，恰有 $\lambda$ 个区组与在 $T$ 中的所有点关联.

216 因此，所有的区组有相同的规模，而且点集的每个 $t$-子集都包含在相同数目的区组中. 有两种不同的记号广泛用于这样的设计，即 $t$-$(v, k, \lambda)$设计和 $S_\lambda(t, k, v)$，两者我们都将使用. 一个施泰纳(Steiner)系 $S(t, k, v)$是 $\lambda=1$ 的 $t$-设计，并且在表示 $S_\lambda(t, k, v)$中略去指标 $\lambda$. 早期的设计理论大多起源于统计学，其中 2-设计用于统计分析的实验设计. 这些设计经常称为平衡不完全区组设计(BIBD). 通常，平凡的设计在该理论中被排除：一个区组包含所有点的设计或者点集的所有 $k$-子集($t\leqslant k$)作为区组的设计，当然是 $t$-设计，但不令人感兴趣.

下面给出几个例子，后面有更多的例子.

**例 19.1** 设$\mathbb{F}_2^4$的非零向量是点. 取满足 $\mathbf{x}+\mathbf{y}+\mathbf{z}=\mathbf{0}$ 的所有三元组$\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$为区组. $\mathbf{x}\neq\mathbf{y}$ 的任意一对 $\mathbf{x}$ 和 $\mathbf{y}$ 唯一地确定第三个元素 $\mathbf{z}$，$\mathbf{z}$ 与 $\mathbf{x}$ 和 $\mathbf{y}$ 都不同，它们满足这一方程. 于是，我们已构建了一个 $S(2, 3, 15)$. 区组是$\mathbb{F}_2^4$的除去 $\mathbf{0}$ 的 2-维子空间.

通过取所有的向量作为点集，并定义满足 $\mathbf{w}+\mathbf{x}+\mathbf{y}+\mathbf{z}=\mathbf{0}$ 的四元组$\{\mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}\}$为区组，构建第二个设计. 这定义了一个 $S(3, 4, 16)$. 注意，如果取含 $\mathbf{0}$ 的区组并删去这个向量，可以找到前一个设计中的区组.

**例 19.2** 取 $K_5$ 的 10 条边作为点集. 在图 19.1 中显示的三类四元组中的每一个是一个区组.

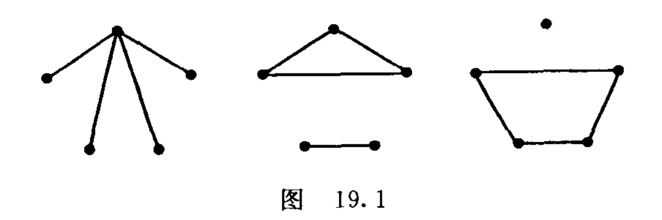


图 19.1

有 5+10+15=30 个区组. 没有(边的)三元组包含在多个区组中. 因此区组包含 120 个

217 不同的三元组，即所有三元组. 我们已构建了一个 $S(3, 4, 10)$.

**例 19.3** 设 $H$ 是阶为 $4k$ 的规范化阿达马矩阵. 删去第一行和第一列. 现在把点与这个矩阵的行等同起来. 每一列定义行的一个子集，即该列中+号对应的那些行. 这些子集是区组. 由定理 18.1 的论证，我们看到任意一对点恰好包含在 $k-1$ 个区组中，且显然所有区组的规模为 $2k-1$. 于是有一个2-$(4k-1, 2k-1, k-1)$设计，这样的设计称为阿达马 2-设计.

考虑同一个矩阵 $H$，但是现在只删去第一行. 其余的每一行确定列集的两个 $2k$-子集. 即使改变行的符号，也不影响这一划分. 定理 18.1 的论证现在表明，对任意三列，恰有 $k-1$ 个子集有这些列中的三个元素. 于是，这些 $2k$-集合是称为阿达马 3-设计的一个3-$(4k, 2k, k-1)$设计的区组.

**例 19.4** 考虑阶为 $4u^2$ 的一个正则阿达马矩阵(见例 18.2). 如果用 1 代替+，用 0 代替−，就得到在每一行和每一列中有 $2u^2+u$ 个 1 的(0, 1)-矩阵，而且每两行或两列的内积为 $u^2+u$. 设列是在 $4u^2$ 个点上的一个设计的区组的特征函数. 该矩阵的性质证明这是一个2-$(4u^2, 2u^2+u, u^2+u)$设计. 人们通常喜欢考虑这一设计的补，即一个 2-$(4u^2, 2u^2-u,$

$u^2-u$)设计.

**问题 19A**　按例 19.2 的风格，这里是另外两个例子.

(i)取 $K_6$ 的边作为一个关联结构的点. 区组是三条边的所有集合，三条边或者是一个完美匹配的边，或者是一个三角形的边. 证明这是一个 $S(2,3,15)$，再证明它与例 19.1 中的设计同构.

(ii)取 $K_7$ 的边作为一个关联结构的点. 区组是三种类型的五条边的所有集合：(a)有一个公共顶点的五条边的"爪"，(b)五边形子图的边集，(c)构成一个三角形和两条不相交的边的五条边. 证明这是一个 $S_3(3,5,21)$.

下面给出 $t$-设计的两个基本定理.

218

**定理 19.2**　一个 $S_\lambda(t,k,v)$的区组数是

$$b=\lambda\binom{v}{t}\Big/\binom{k}{t}. \tag{19.1}$$

**证明**　以两种方式对$(T,B)$对的数目进行计数，其中 $T$ 是$\mathcal{P}$的一个$t$-子集且 $B$ 是与 $T$ 的所有点关联的一个区组，我们发现 $\lambda\binom{v}{t}=b\binom{k}{t}$. ■

**定理 19.3**　给定 $i$，$0\leqslant i\leqslant t$，与$\mathcal{P}$的一个 $i$-子集 $I$ 的所有点关联的区组数是

$$b_i=\lambda\binom{v-i}{t-i}\Big/\binom{k-i}{t-i}. \tag{19.2}$$

这就是说，对 $i\leqslant t$ 每个 $S_\lambda(t,k,v)$也是一个 $i$-设计.

**证明**　以两种方式对$(T,B)$对的数目进行计数，其中 $T$ 是$\mathcal{P}$的一个包含 $I$ 的 $t$-子集且 $B$ 是 $T$ 的所有点关联的一个区组. ■

**推论**　如果$\mathcal{D}$是点集$\mathcal{P}$和区组集$\mathcal{B}$的一个 $t$-设计，且 $I$ 是$\mathcal{P}$的一个满足 $|I|\leqslant t$ 的子集，那么点集$\mathcal{P}\setminus I$和区组$\{B\setminus I: I\subseteq B\}$构成一个 $S_\lambda(t-i,k-i,v-i)$. 这个设计称为导出设计$\mathcal{D}_I$.

在例 19.1 中，我们已经看到过导出设计的一个例子. 如果取 $I=\{\mathbf{0}\}$，$S(3,4,16)$的导出设计是 $S(2,3,15)$.

**问题 19B**　证明：如果 $S(3,6,v)$存在，则 $v\equiv 2$ 或 $6 \pmod{20}$.

与任意一个点(例如 $b_1$)关联的区组数通常用 $r$(重复数)表示. 定理 19.3 的两种特殊情形是 2-设计的参数的如下关系：

$$bk=vr, \tag{19.3}$$

$$\lambda(v-1)=r(k-1). \tag{19.4}$$

219

**定理 19.4**　设 $0\leqslant j\leqslant t$. 与$\mathcal{P}$的一个 $j$-子集 $J$ 中的任何一点都不关联的一个 $S_\lambda(t,k,v)$的区组数是

$$b^j=\lambda\binom{v-j}{k}\Big/\binom{v-t}{k-t}. \tag{19.5}$$

**证明**　对 $x\in\mathcal{P}$，设$\mathcal{B}_x$是与 $x$ 关联的区组的集合. 根据定理 10.1，即容斥原理，可以发现

$$b^j=\sum_{i=0}^{j}(-1)^i\binom{j}{i}b_i.$$

定理的结果通过(19.2)的代入，然后利用(10.5)得到.

观察到 $b^j$ 显然不依赖特定的集合 $J$，并用两种方式对$(J, B)$进行计数会更快一些，这里 $J$ 是$\mathcal{P}$的一个 $j$-子集且 $J\cap B=\varnothing$. 于是，$\binom{v}{j}b^j=b\binom{v-k}{j}$. 然后，由定理 19.2 得到本定理的结果. ■

**推论** 如果 $i+j\leqslant t$，则 $S_\lambda(t, k, v)$中的区组数是一个常数

$$b_i^j=\lambda\frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}},\tag{19.6}$$

这些区组中的每一个与 $i$ 个点的一个集合的所有点关联且不与不相交的 $j$ 个点的一个集合的任何一点关联.

**证明** 应用定理 19.4 于$(t-i)$-设计$\mathcal{D}_I$可得到推论的结果，这里 $I$ 是 $i$ 个点的集合. ■

**推论** 如果 $J$ 是$\mathcal{P}$的一个$j$-子集，$j\leqslant t$，则点集$\mathcal{P}\setminus J$ 和满足$B\cap J=\varnothing$的区组 $B$ 构成一个 $S_\mu(t-j, k, v-j)$，称之为剩余设计$\mathcal{D}^J$.

**问题 19C** (i)证明满足 $v\leqslant k+t$ 的 $S_\lambda(t, k, v)$是平凡的. (ii)证明满足 $v\geqslant k+t$ 的 $S_\lambda(t, k, v)$的补是一个 $t$-设计，确定其参数.

[220] **例 19.5** 考虑阿达马 3-设计 3-$(4k, 2k, k-1)$，相对于一个点的一个集合构成剩余设计. 可以找到一个阿达马 2-设计 2-$(4k-1, 2k, k)$，即例 19.3 的设计的补.

存在一个 $S_\lambda(t, k, v)$的显然的必要条件是(19.2)中的 $b_i$ 是整数. 然而，这个条件不是充分的. 不存在 $S(10, 16, 72)$，正如下面的定理所证明的，它属于 Tits(1964).

**定理 19.5** 在任何一个非平凡的施泰纳系 $S(t, k, v)$中，

$$v\geqslant(t+1)(k-t+1).$$

**证明** 在一个施泰纳系中，任意两个不同的区组至多有 $t-1$ 个公共点. 选择不包含在任意区组中的一个有 $t+1$ 个点的集合 $S$，对满足 $|T|=t$ 的每一个集合 $T\subseteq S$，有唯一一个包含 $T$ 的区组 $B_T$. 每个这样的 $B_T$ 与不在 $S$ 中的 $k-t$ 个点关联，不在 $S$ 中的任意一点至多与一个这样的区组 $B_T$ 关联，原因是两个这样的区组已经有 $S$ 中的 $t-1$ 个公共点. 这证明所有区组 $B_T$ 的并包含$(t+1)+(t+1)(k-t)$个点，由此得到定理的结果. ■

给定满足 $|\mathcal{P}|=v$ 且 $|\mathcal{B}|=b$ 的一个关联结构，关联矩阵 $N$ 是行由$\mathcal{P}$的元素 $p$ 指示. 列由$\mathcal{B}$的元素 $B$ 指示的 $v\times b$ 矩阵，如果 $p$ 与 $B$ 关联，项 $N(p, B)=1$；否则，$N(p, B)=0$. 注意，在 $NN^\top$ 的 $p$ 行 $q$ 列的项是遍历所有区组 $B$ 的 $N(p, B)N(q, B)$之和，这是既包含 $p$ 又包含 $q$ 的区组的数目. 对偶地，在 $N^\top N$ 的 $A$ 行 $B$ 列的项是 $A\cap B$ 的基数.

如果有两个置换矩阵 $P$ 和 $Q$ 使得 $N'=PNQ$，则关联矩阵为 $N$ 和 $N'$的两个设计$\mathcal{D}$和$\mathcal{D}'$称为同构的或等价的.

我们以后常把 $N$ 与设计等同，即用作为区组的列代替作为区组的特征函数的列.

现在，如果 $N$ 是一个 2-设计的关联矩阵，则 $NN^\top$ 在对角线上各处的项为 $r$，在其他所有位置的项为 $\lambda$，即

$$NN^{\top} = (r-\lambda)I + \lambda J, \tag{19.7}$$

这里 $I$ 和 $J$ 是 $v \times v$ 矩阵．

221

**问题 19D**　设 $N$ 是具有下列性质的 $11\times 11$ 阶(0，1)-矩阵：(i) $N$ 的每行有六个 1；(ii) $N$ 的任意两行的内积至多为 3．证明 $N$ 是 2-(11，6，3)设计的关联矩阵．此外，证明这个设计是唯一的(在同构意义上)．

下面的定理以费希尔(Fisher)不等式著称．

**定理 19.6**　对有 $b$ 个区组且 $v>k$ 的 2-$(v, k, \lambda)$设计，我们有

$$b \geqslant v.$$

**证明**　因为 $v>k$，由(19.4)有 $r>\lambda$．因为 $J$ 有一个特征值 $v$ 且它的其他特征值为 0，所以(19.7)右边的矩阵有 $v-1$ 个特征值 $(r-\lambda)$ 和一个特征值 $(r-\lambda)+\lambda v=rk$．于是它的行列式 $rk(k-\lambda)^{v-1}\neq 0$ 且 $N$ 的秩为 $v$．这蕴涵着 $b\geqslant v$． ■

从上面的论证，可以得出一个非常重要的结论，在下一定理中给出．

**定理 19.7**　如果有 $b=v$ 个区组且 $v$ 是偶数的一个 2-$(v, k, \lambda)$设计，则 $k-\lambda$ 必为一个平方数．

**证明**　因为 $b=v$，我们有 $r=k$，现在 $N$ 是一个 $v\times v$ 矩阵且由(19.7)

$$(\det N)^2 = k^2(k-\lambda)^{v-1}.$$

因为 $\det N$ 是一个整数，所以完成了证明． ■

定理 19.6 由 A. Ya. Petrenjuk(1968)对满足 $v\geqslant k+2$ 的任意 $S_\lambda(4, k, v)$推广到 $b\geqslant \binom{v}{2}$，并最终由 Ray-Chaudhuri and Wilson(1975)推广到任意的 $t$-设计．

**定理 19.8**　对满足 $t\geqslant 2s$ 且 $v\geqslant k+s$ 的 $S_\lambda(t, k, v)$，我们有 $b\geqslant \binom{v}{s}$．

**证明**　我们引入 $t$-设计 $\mathcal{D}=S_\lambda(t, k, v)$的高度关联矩阵．对 $i=0, 1, 2, \cdots$，设 $N_i$ 表示 $\binom{v}{i}\times b$ 矩阵，该矩阵的行由点的 $i$-元素子集指示，列由区组指示．如果 $Y\subseteq B$，在 $Y$ 行 $B$ 列的项为 1；否则为 0．对 $0\leqslant i\leqslant j\leqslant v$，我们用 $W_{ij}$ 表示关联结构的第 $i$ 个关联矩阵，该关联结构的区组是一个 $v$-集合的所有 $j$-元素子集．于是 $W_{ij}$ 是一个 $\binom{v}{i}\times\binom{v}{j}$矩阵．

222

我们断言

$$N_sN_s^{\top} = \sum_{i=0}^{s} b_{2s-i}^{i} W_{is}^{\top} W_{is}.$$

为明白这一点，注意到 $N_sN_s^{\top}$的行由点的 $s$-元素子集 $E$ 指示，列由点的 $s$-元素子集 $F$ 指示，对给定的 $E$ 和 $F$，在 $N_sN_s^{\top}$的 $E$ 行 $F$ 列的项是既包含 $E$ 又包含 $F$ 的区组的数目．这个数目是 $b_{2s-\mu}$，其中 $\mu := |E\cap F|$．在 $W_{is}^{\top}W_{is}$的 $E$ 行 $F$ 列的项是既包含在 $E$ 中又包含在 $F$ 中的点的 $i$-子集的数目，即$\binom{\mu}{i}$．于是上面方程右侧的$(E, F)$-项是 $\sum_{i=1}^{s} b_{2s-i}^{i}\binom{\mu}{i}$，由(19.6)得出该项

是 $b_{2s-\mu}$.

$\binom{v}{s}\times\binom{v}{s}$阶矩阵 $b^{i}_{2s-i}W^{\top}_{is}W_{is}$ 都是半正定的，因为 $b^{s}_{s}>0(v\geqslant k+s)$，所以 $b^{s}_{s}W^{\top}_{ss}W_{ss}=b^{s}_{s}I$ 是正定的．因此 $N_sN^{\top}_s$是正定的且因此非奇异．$N_sN^{\top}_s$的秩等于 $N_s$ 的秩，即 $N_s$ 的秩为$\binom{v}{s}$，$\binom{v}{s}$不超过 $N_s$ 的列数 $b$． ■

在 Wilson-Petrenjuk 不等式中，即定理 19.8 中如果等式成立，则称 $2s$-设计是*紧的*．我们仅知的满足 $s>1$ 且 $v>k+s$ 的例子是唯一的施泰纳系 $S(4, 7, 23)$及其补，将在下一章讨论这个施泰纳系．

给出 $t$-设计历史中的观念是有用的．现在只知道有限多个满足 $t\geqslant 4$ 的施泰纳系．最著名的是由 E. Witt(1938)发现的设计 $S(5, 8, 24)$、$S(5, 6, 12)$以及导出的 4-设计．这些将在下一章中介绍．R. H. F. Denniston(1976)构造了 $S(5, 6, 24)$，$S(5, 7, 28)$，$S(5, 6, 48)$和 $S(5, 6, 84)$．W. H. Mills(1978)构造了 $S(5, 6, 72)$．此外，这些施泰纳系的导出设计是施泰纳系．M. J. Granell and T. S. Griggs(1994)构造了 $S(5, 6, 108)$．从那以后，还没有发现其他施泰纳系．1972 年，W. O. Alltop 构造了第一个没有重复区组的 5-设计的无穷序列．我们 [223] 注意到容易证明，对任意 $t$，存在带重复区组的 $t$-设计，但很长一段时间，设计理论家认为对 $t>6$ 不存在没有重复区组的非平凡 $t$-设计．1982 年，D. W. Leavitt 和 S. S. Magliveras 发现了第一个简单的 6-设计，且在 1986 年，D. L. Kreher 和 S. P. Radziszowski 发现了最小可能的简单 6-设计 $S_4(6, 7, 14)$．在这个领域引起很大轰动的是 L. Teirlinck(1987)的论文，文中证明对所有 $t$，存在非平凡的 $t$-设计．他构造的设计有巨大的参数，因此小例子的构造仍是一个未解决的问题．对一些特殊的参数集，已证明对应的设计不存在．

在本章余下的部分，我们主要讨论 2-设计．当 $t=2$ 时，在"$t$-$(v, k, \lambda)$"记号中我们经常省略 2 而简记成$(v, k, \lambda)$-设计．

一类特别有趣的设计是满足 $b=v$ 的 2-设计．在这种情形，设计的关联矩阵 $N$ 是一个方阵，这些设计称为*正方形设计*．然而，容易引起混淆的名字*对称设计*却是标准术语．（注意 $N$ 不必是对称的．）对一个对称的 2-$(v, k, \lambda)$设计，(19.4)变成

$$\lambda(v-1)=k(k-1).$$

一些作者使用*射影设计*这一名字，它源自满足 $b=v$ 的 2-$(v, k, 1)$设计称为射影平面(见例 19.7)．我们对这一名字不满意，对这些设计我们使用术语*对称设计*．

**问题 19E** 设$\mathcal{D}$是有 $b$ 个区组且通过每个点有 $r$ 个区组的 2-$(v, k, \lambda)$设计．设 $B$ 为任意一个区组．证明与 $B$ 相交的区组数至少是

$$k(r-1)^2/[(k-1)(\lambda-1)+(r-1)].$$

证明相等性成立，当且仅当与 $B$ 相交的任何一个区组与它相交于常数个点．

**例 19.6** 取$\mathbb{Z}_7$ 的元素作为点，且对 $x\in\mathbb{Z}_7$，所有的三元组 $B_x:=\{x, x+1, x+3\}$作为区组．容易检验这是一个 $S(2, 3, 7)$． [224] 通常如图 19.2 所示．线代表区组，但是有一个区组一定要用圆圈

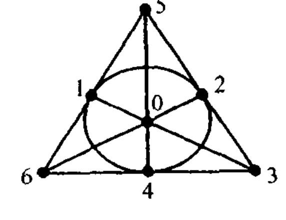



图 19.2

表示.

这个设计以费诺(Fano)平面著称. 构造该设计的想法将在第27章扩展. 它依赖的事实是,$\{0, 1, 3\}$的元素之间的六个差恰是$\mathbb{Z}_7$中的所有非零元素. 如果我们希望找到包含比如说$\{1, 6\}$的区组,观察到$6-1=1-3$,因此取$x=5$并发现$x+1=6$,$x+3=1$,即这个数对确实在$B_5$中. 读者按相同方式利用$\mathbb{Z}_{13}$,不难找到一个$S(2, 4, 13)$.

$\lambda=1$的对称设计称为*射影平面*. 如果$k$是区组的规模,则$n=k-1$称为该平面的阶(为何这样做将在例19.7中讲解). 用$n$表示,阶为$n$的射影平面的参数是:

$$v = n^2+n+1, \qquad k = n+1, \qquad \lambda = 1.$$

区组通常称为线. 费诺平面是(唯一的)阶为2的射影平面.

**例 19.7** 考虑向量空间$\mathbb{F}_q^3$. 这个向量空间包含$(q^3-1)/(q-1)=q^2+q+1$个1-维子空间和同样数目的2-维子空间. 现在我们构造一个关联结构$(\mathcal{P}, \mathcal{B}, I)$,这里$\mathcal{P}$和$\mathcal{B}$是$\mathbb{F}_q^3$的两类子空间. 如果一个1-维子空间包含在一个2-维子空间内,我们说它们是关联的. 显然这样我们已定义了一个阶为$q$的射影平面,即一个$2\text{-}(q^2+q+1, q+1, 1)$设计. 这个设计通常用$PG(2, q)$或$PG_2(q)$表示,它表示2维$q$阶的射影几何. [225]

如果用$\mathbb{R}$代替$\mathbb{F}_q$也可应用上面定义的构造. 那么我们得到经典的实射影平面,其中点是1-维子空间且线是2-维子空间,这种几何与经典射影几何在没有两条线是平行的这一事实上形成对照. 当谈及上面定义的设计时,我们使用几何学术语.

**问题 19F** 寻找$\mathbb{Z}_{21}$的一个子集$S=\{s_1, \cdots, s_5\}$,使得$\mathbb{Z}_{21}$的元素作为点和21个区组$S+x(x\in\mathbb{Z}_{21})$形成4阶射影平面. (提示:对$2S=S$有一个解$S$.)

**问题 19G** 设$(R, C, S; L)$是阶为6的拉丁方. 定义$\mathcal{P}:=R\times C$. 设$\mathcal{B}$为区组的集合:

$$B_{ij} := \{(x,y)\in R\times C : x=i \quad 或 \quad y=j \quad 或 \quad L(x,y)=L(i,j)\}\setminus\{(i,j)\}$$
$$对 (i,j)\in R\times C.$$

(1)证明这定义了一个$2\text{-}(36, 15, 6)$设计.

(2)证明存在阶为36的正则阿达马矩阵.

**问题 19H** 设$\mathcal{D}$是一个$3\text{-}(v, k, \lambda)$设计. 假设$\mathcal{D}$相对于一点$p$的导出设计(即在定理19.3的推论中$i=1$的情形)是一个对称设计.

(1)证明$\lambda(v-2)=(k-1)(k-2)$.

(2)证明$\mathcal{D}$的任意两个区组在0个或$\lambda+1$个点相交.

(3)证明不在区组$B$中的点集与和$B$不相交的区组一起形成一个2-设计$\mathcal{D}^B$.

(4)将费希尔不等式应用于设计$\mathcal{D}^B$,导出$v=2k$,或者$k=(\lambda+1)(\lambda+2)$,或者$k=2(\lambda+1)(\lambda+2)$.

设计$\mathcal{D}$的可能性是什么?我们知道有这些性质的设计吗?

**问题 19I** 设$O$是阶为$n$的一个射影平面的点的子集,使得$O$中没有三个点在一条线上. 证明:如果$n$是奇数,$|O|\leqslant n+1$;如果$n$为偶数,$|O|\leqslant n+2$. 没有三个点在一条线上的$n+1$个点的集合称为*卵形*;没有三个点在一条线上的$n+2$个点的集合称为*超卵形*. $PG_2(4)$的两个构造已在例19.7和问题19F中给出. 在每一情形,构造一个超卵形. [226]

**问题 19J** 在 $PG_2(q)(q=2^m)$中，设 $O$ 为(有 $n+2$ 个点的)超卵形. 任何 $q^2-1$ 个点$p\notin O$ 具有 $O$ 恰好有$\frac{1}{2}(q+2)$条割线通过 $p$ 的性质. 在 $O$ 中取五个点并把它们分割成

$$\{\{p_1,p_2\},\{p_3,p_4\},\{p_5\}\}.$$

共有 15 种分割方式. 两个对确定交于一个点 $p\notin O$ 的两条割线. 通过 $p$ 和 $p_5$ 的线交于 $O$ 中一个点，记为 $p_6$. 这定义了 15 个(不必不同)$O$ 中包含给定五个点的点的六元组. 这种做法定义一个 $S_\lambda(5, 6, q+2)$，该构造属于 D. Jungnickel and S. A. Vanstone(1987). 证明"坐标"(如在例 19.7 中)为$(1, t, t^2)(t\in\mathbb{F}_q)$的点，与$(0, 1, 0)$和$(0, 0, 1)$形成 $PG_2(q)$中的超卵形 $O$. 证明 $O$ 中 $p_1$ 到 $p_5$ 的一个适当的选择和上面解释的构造法产生重复区组，即这个 5-设计不是简单的.

2-$(n^2, n, 1)$设计称为*仿射平面*. 平面(=2-维向量空间)$\mathbb{F}_q^2$的点和线形成阶为 $q$ 的仿射平面. 对这样的设计我们采用记号 $AG_2(n)$(阶为 $n$ 的 2-维仿射几何).

**例 19.8** 设$\mathcal{D}$为 $n$ 阶射影平面. 如果删去一条线和线上的所有点，可以找到阶为 $n$ 的一个仿射平面.

**问题 19K** 设$\mathcal{D}$为任意一个 $n$ 阶仿射平面. 如果 $B_1$ 和 $B_2$ 是两个区组，它们相同或者没有公共点，那么就写作 $B_1\sim B_2$. 证明$\sim$是一个等价关系. 这个关系的一个类称为*平行类*. 证明存在一个 $n$ 阶的射影平面使得$\mathcal{D}$能从例 19.8 中构建的平面得到.

227

现在我们证明，如果 $N$ 是一个对称设计$\mathcal{D}$的关联矩阵，则 $N^\top$ 也是一个对称设计$\mathcal{D}^\top$的关联矩阵，$\mathcal{D}^\top$ 称为$\mathcal{D}$的对偶.

**定理 19.9** *设 $N$ 为一个对称 2-$(v, k, \lambda)$设计的关联矩阵，那么 $N^\top$ 也是一个设计的关联矩阵.*

**证明** 考虑该设计的任何一个区组 $B$. 对 $0\leqslant i\leqslant k$，设 $a_i$ 是与 $B$ 有 $i$ 个公共点的区组($\neq B$)数. 然后对区组、满足 $p\in B\cap B'$的对$(p, B')$以及满足 $p\neq q$ 且$\{p, q\}\subseteq B\cap B'$的三元组$(p, q, B')$进行计数，可以发现：

$$\sum_{i=0}^{k}a_i=v-1,\quad \sum_{i=0}^{k}ia_i=k(k-1),\quad \sum_{i=0}^{k}\binom{i}{2}a_i=\binom{k}{2}(\lambda-1),$$

由此得到 $\sum\limits_{i=0}^{k}(i-\lambda)^2a_i=0$. 所以，任意区组 $B'\neq B$ 与 $B$ 都有 $\lambda$ 个公共点，即 $N^\top N=(k-\lambda)I+\lambda J$.

■

注意，在例 19.7 中，我们不需要指出集合$\mathcal{P}$是 1-维子空间或 2-维子空间. 在后一种情形，我们有前一种情形的对偶.

在许多情形，设计$\mathcal{D}$和$\mathcal{D}^\top$不是同构的.

设$\mathcal{D}$是一个对称的 2-$(v, k, \lambda)$设计，有两种其他的方式从$\mathcal{D}$得到一个设计. 这两种设计称为$\mathcal{D}$的导出设计和剩余设计. 这与我们已经引入的术语有些混淆. 此后我们总指明两者的意义. 取$\mathcal{D}$的任意一个区组 $B$. $\mathcal{D}$相对于 $B$ 的剩余以$\mathcal{P}\setminus B$ 作为点集，而以满足 $B'\neq B$ 的所有 $B'\setminus B$ 作为区组. 它是一个 2-$(v-k, k-\lambda, \lambda)$设计. $\mathcal{D}$的导出设计以 $B$ 作为点集，而以满足 $B'\neq B$ 的所有$B'\cap B$作为区组. 它是一个 2-$(k, \lambda, \lambda-1)$设计. 如果参数为 $v$, $k$, $b$, $r$, $\lambda$ 的

设计是一个对称设计的剩余，则 $r=k+\lambda$. 任何一个使这个等式成立的 2-设计称为拟剩余设计. 如果这样的设计不是对称设计的剩余，那么我们就说它是不可嵌入的. 问题 19K 的断言是每个仿射平面可嵌入在一个射影平面中. W. S. Connor(1952)的一个定理断言，每个 $\lambda=2$ 的拟剩余设计是可嵌入的，这个定理将在第 21 章讨论.

228

**例 19.9**　设 $C:=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}$，再设 $E_i$ 表示在 $i$ 列是 1、其他地方都是 0 的 3×3 矩阵，则

$$N:=\begin{bmatrix}E_1&I&I&I\\E_2&I&C&C^2\\E_3&I&C^2&C\end{bmatrix}$$

是 $AG_2(3)$的 9×12 关联矩阵. 定义

$$A:=\begin{bmatrix}1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\\1\,1\,1\,0\,0\,0\,1\,1\,1\,0\,0\,0\\1\,1\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1\\0\,0\,0\,1\,1\,1\,1\,1\,1\,0\,0\,0\\0\,0\,0\,1\,1\,1\,0\,0\,0\,1\,1\,1\\0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\end{bmatrix},\quad B:=\begin{bmatrix}1\,1\,0\,0\\1\,1\,0\,0\\1\,1\,0\,0\\1\,0\,1\,0\\1\,0\,1\,0\\1\,0\,1\,0\\1\,0\,0\,1\\1\,0\,0\,1\\1\,0\,0\,1\end{bmatrix}.$$

形成 24×16 矩阵

$$D:=\begin{bmatrix}A&O\\N&B\\N&J-B\end{bmatrix}.$$

容易验证$\mathcal{D}^{\top}$是 2-(16，6，3)设计的 16×24 关联矩阵. 这是一个拟剩余设计，然而，它不可能是 2-(25，9，3)对称设计的剩余，因为对 $1\leqslant i\leqslant 9$，$\mathcal{D}$的 $i+6$ 行和 $i+15$ 行的内积等于 4，由定理 19.9，2-(25，9，3)设计的关联矩阵的列的内积等于 3. 这证明存在 $\lambda=3$ 的不可嵌入设计.

我们用于证明定理 19.9 的计数论证和适当的二次型的组合广泛地用于组合学中. 然而，有时用代数方法更容易，正如下面的定理中所显示的，这个定理属于 Ryser.（读者可以尝试用计数论证证明该定理.）

229

**定理 19.10**　设$\mathcal{D}=(\mathcal{P},\mathcal{B},\boldsymbol{I})$是满足 $|\mathcal{P}|=|\mathcal{B}|=v$. 区组规模为 $k$ 的关联结构，使得任意两个区组交于 $\lambda$ 个点. 那么$\mathcal{D}$是一个对称的 2-设计.

**证明**　设 $N$ 是$\mathcal{D}$的关联矩阵，则

$$N^{\top}N=(k-\lambda)I+\lambda J,\tag{19.8}$$

以及

$$JN=kJ.\tag{19.9}$$

由定理 19.9，如果我们能证明 $NJ=kJ$，就完成了证明. 由(19.8)可以看到 $N$ 是非奇异的，且因此(19.9)可以写成 $J=kJN^{-1}$. 从(19.8)可以发现 $JN^{\top}N=(k-\lambda+\lambda v)J$，所以

$$JN^{\top} = (k-\lambda+\lambda v)JN^{-1} = (k-\lambda+\lambda v)k^{-1}J,$$

即 $N$ 的列和为常数. 那么，这些列和一定是 $k$. 这就证明了定理，并得出 $(k-\lambda+\lambda v)k^{-1}=k$，正如由(19.3)和(19.4)所预期的. ■

作为对最著名的关于设计的不存在性定理的准备，我们需要两个结果，它们属于拉格朗日(Lagrange). 第一个结果，考虑 $n=1$ 时(18.6)的矩阵 $H$，即 $A_i=(a_i)$. 由 $\boldsymbol{y}:=\boldsymbol{x}H$ 定义 $\boldsymbol{y}=(y_1, y_2, y_3, y_4)$，这里 $\boldsymbol{x}=(x_1, x_2, x_3, x_4)$. 则由(18.7)可以发现

$$(a_1^2+a_2^2+a_3^2+a_4^2)(x_1^2+x_2^2+x_3^2+x_4^2) = (y_1^2+y_2^2+y_3^2+y_4^2). \qquad (19.10)$$

利用这个恒等式，拉格朗日证明每个整数是四个平方数之和. 显然，这个等式表明对素数加以证明就够了. 对素数是四个平方数之和的一个简洁证明，可参考 Chandrasekharan(1968).

下面的不存在性定理以 Bruck -Ryser-Chowla 定理著称.

**定理 19.11** *如果 $v$，$k$，$\lambda$ 是使得 $\lambda(v-1)=k(k-1)$ 的整数，则对一个对称 2-$(v, k, \lambda)$ 设计的存在性，下列条件是必要的：*

*(i)如果 $v$ 为偶数，则 $k-\lambda$ 是一个数的平方.*

230

*(ii)如果 $v$ 是奇数，则方程 $z^2=(k-\lambda)x^2+(-1)^{(v-1)/2}\lambda y^2$ 有不全为零的整数解 $x$，$y$，$z$.*

**证明** 断言(i)在定理 19.7 中已被证明. 因此假定 $v$ 是奇数. 设 $\mathcal{D}$ 是关联矩阵 $N=(n_{ij})$ 的对称 2-$(v, k, \lambda)$ 设计，令 $n:=k-\lambda$. 现在我们由

$$L_i := \sum_{i=1}^{v} n_{ij}x_j, \qquad 1\leqslant i\leqslant v$$

引入 $v$ 个以 $x_1$，…，$x_v$ 为变量的线性型 $L_i$. 那么方程 $N^{\top}N=(k-\lambda)I+\lambda J$ 蕴涵

$$L_1^2+\cdots+L_v^2 = n(x_1^2+\cdots+x_v^2)+\lambda(x_1+\cdots+x_v)^2. \qquad (19.11)$$

由拉格朗日定理，$n$ 可以写成 $n=a_1^2+\cdots+a_4^2$. 这个式子和(19.11)允许我们取变量 $x_j$ 中的四个并写成

$$n(x_i^2+x_{i+1}^2+x_{i+2}^2+x_{i+3}^2) = (y_i^2+y_{i+1}^2+y_{i+2}^2+y_{i+3}^2), \qquad (19.12)$$

其中每个 $y_j$ 是四个变量 $x_i$，…，$x_{i+3}$ 的线性型.

我们首先假设 $v\equiv1 \pmod 4$. 通过把这个结果用于(19.11)，每次四个变量，再引入 $w$ 表示 $x_1+\cdots+x_v$，(19.11)化为

$$L_1^2+\cdots+L_v^2 = y_1^2+\cdots+y_{v-1}^2+nx_v^2+\lambda w^2. \qquad (19.13)$$

因为在(18.6)中 $H$ 是可逆的，对 $1\leqslant j\leqslant v-1$，我们可把变量 $x_j$ 表示成对应的 $y_j$ 的线性型，因此，$w$ 是这些变量和 $x_v$ 的线性型. 其次，按如下方法减少变量的数目：对 $y_1$，…，$y_{v-1}$，$x_v$ 表示的线性型 $L_1$，如果 $y_1$ 的系数不是 $+1$，则设 $L_1=y_1$；如果 $y_1$ 的系数是 $+1$，则设 $L_1=-y_1$. 在这两种情形，我们把 $y_1$ 作为其余变量 $y_j$ 和 $x_v$ 的一个线性表示来解方程. 这也代入 $w$ 的表达式中. 于是(19.11)化为

$$L_2^2+\cdots+L_v^2 = y_2^2+\cdots+y_{v-1}^2+nx_v^2+\lambda w^2.$$

对 $y_2$，…，$y_{v-1}$按这种方式进行．在每一步，$w$ 被剩余变量的其他线性型所代替，因此以

$$L_v^2 = nx_v^2 + \lambda w^2$$

231

结束，其中 $L_v$ 和 $w$ 都是变量 $x_v$ 的有理数倍．如果这个等式乘以因子的公分母，则得到一个整数方程

$$z^2 = (k-\lambda)x^2 + \lambda y^2.$$

这就证明了 $v\equiv 1 \pmod 4$时的断言．如果 $v\equiv 3 \pmod 4$，可以在(19.13)的两端加上 $nx_{v+1}^2$之后，再采用同样的过程，这里 $x_{v+1}$是一个新变量．方程最终约化为 $nx_{v+1}^2 = y_{v+1}^2 + \lambda w^2$，如果再乘以因子的公分母，则得到符合断言(ii)的类型为

$$(k-\lambda)x^2 = z^2 + \lambda y^2$$

的方程． ■

**例 19.10** 从例 19.7 我们知道，对 $2\leqslant n\leqslant 9$，存在阶为 $n$ 的射影平面，但 $n=6$ 可能是例外．由定理 19.11，存在阶为 6 的射影平面的必要条件是方程 $z^2=6x^2-y^2$ 有非平凡解．如果存在这样的一组解，那么也存在 $x$，$y$ 和 $z$ 没有公共素因子的解，即 $z$ 和 $y$ 都是奇数．那么 $z^2$ 和 $y^2$ 都$\equiv 1 \pmod 8$．因为 $6x^2 \pmod 8$要么是 0，要么是 6，我们看到该方程只有平凡解(0，0，0)．所以不存在阶为 6 的射影平面．

如果对阶为 10 的平面进行尝试，可以发现方程 $z^2=10x^2-y^2$ 有解 $x=1$，$y=1$，$z=3$．在这种情形，定理 19.11 没有给出结论．1989 年，Lam 等人宣布，在 Cray 1 上进行几百小时的计算机搜索排除了阶为 10 的射影平面的存在性，这是到目前为止不使用定理 19.11 来讨论对称2-设计的不存在性的唯一情形．

**推论** *如果存在阶 $n\equiv 1$ 或 $2 \pmod 4$的射影平面，则 $n$ 为两个整数的平方之和．*

**证明** 条件 $n\equiv 1$ 或 $2 \pmod 4$蕴涵 $v=n^2+n+1\equiv 3 \pmod 4$．定理 19.11 断言 $n$ 是两个有理数的平方之和．众所周知 $n$ 是两个有理数的平方之和当且仅当 $n$ 是两个整数的平方之和．(这个论断由 $n$ 是两个整数的平方之和当且仅当 $n$ 的非平方部分的素因子不是$\equiv 3 \pmod 4$得出．)

232

**问题 19L** 证明对称 2-(29，8，2)设计不存在．

**问题 19M** 假定 $M$ 是一个阶为 $v$ 的有理数方阵且 $MM^{\top}=mI$．证明：如果 $v$ 是奇数，则 $m$ 是一个平方数．证明：如果 $v\equiv 2 \pmod 4$，则 $m$ 是两个有理数的平方之和．

(注意：后一个结论的一个推论是，阶 $n\equiv 2 \pmod 4$的会议矩阵的存在性蕴涵 $n-1$ 是两个平方数之和．)

关于 2-设计的构造已做了许多工作．我们只讨论一些例子，它们给出所用方法的思想．要考虑的最小的非平凡对$(k，\lambda)$是(3，1)．2-$(v，3，1)$设计称为*施泰纳三元系*．用 $STS(v)$ 表示这样的设计．由(19.3)和(19.4)，存在这样的设计的一个必要条件是$v\equiv 1 \pmod 6$或 $v\equiv 3 \pmod 6$．我们将证明这个条件也是充分的．证明通过用例 19.11 和例 19.15 中的直接构造得到．然而，有必要看一下一种更复杂的方法的几个例子．这里的方法可用于不是施泰纳三元系的其他设计的构造．此外，它们能用于产生有特定的子设计(见问题 19N)或指定的自同构群的

设计. 这种方法的思路是寻找小例子的直接构造和一些递归构造，然后对任何满足必要条件的 $v$，利用已知的小例子，通过递归方法证明 $STS(v)$能被构造. 下面我们将看到这事实上约化为一个(不很困难的)数论问题. 如上所述，我们局限在一些例子中，读者可能希望尝试不利用例 19.11 和例 19.15，证明对 $v$ 的所有可能的值，我们的例子对找到$STS(v)$是充分的.

233 考虑只有一个大小为 3 的区组的平凡设计 $STS(3)$. 我们已经看到 $STS(7)=PG_2(2)$和 $STS(9)=AG_2(3)$的构造. 在例 19.1 中，我们已构造了 $STS(15)$.

**例 19.11** 设 $n=2t+1$. 我们定义$\mathcal{P}:=\mathbb{Z}_n\times\mathbb{Z}_3$. 取满足 $x\in\mathbb{Z}_n$ 的所有三元组$\{(x,0),(x,1),(x,2)\}$，以及满足在$\mathbb{Z}_n$ 中 $x\neq y$ 且 $i\in\mathbb{Z}_3$ 的所有三元组$\left\{(x,i),(y,i),\left(\frac{1}{2}(x+y),i+1\right)\right\}$作为区组. 这一简单的构造对任意 $t$ 提供了一个 $STS(6t+3)$.

**例 19.12** 设 $q=6t+1$ 是一个素数幂且 $\alpha$ 为$\mathbb{F}_q$ 中的一个本原元，即$\mathbb{F}_q^*$是由 $\alpha$ 生成的循环群. 定义

$$B_{i,\xi}:=\{\alpha^i+\xi,\alpha^{2t+i}+\xi,\alpha^{4t+i}+\xi\},\qquad 0\leqslant i<t,\quad \xi\in\mathbb{F}_q. \tag{19.14}$$

我们断言$\mathbb{F}_q$ 的元素作为点，与区组 $B_{i,\xi}$构成一个 $STS(q)$. 证明的思路与例 19.6 相同. 注意 $\alpha^{6t}=1,\alpha^{3t}=-1$，再由 $\alpha^s=(\alpha^{2t}-1)$定义 $s$. 考虑来自 $B_{0,0}$的对子的六个差. 它们是:

$$\alpha^{2t}-1=\alpha^s,\qquad -(\alpha^{2t}-1)=\alpha^{s+3t},$$
$$\alpha^{4t}-\alpha^{2t}=\alpha^{s+2t},\qquad -(\alpha^{4t}-\alpha^{2t})=\alpha^{s+5t},$$
$$\alpha^{6t}-\alpha^{4t}=\alpha^{s+4t},\qquad -(1-\alpha^{4t})=\alpha^{s+t}.$$

由此得出，对于$\mathbb{F}_q$ 中的$\eta\neq0$，存在一个唯一的 $i$，$0\leqslant i<t$，使得 $\eta$ 作为 $B_{i,0}$的两个元素的差出现. 因此对$\mathbb{F}_q$ 中的$x$ 和$y$，存在一个唯一的 $i$ 和一个唯一的$\xi\in\mathbb{F}_q$，使得对子 $x$，$y$ 出现在区组 $B_{i,\xi}$中.

例 19.6 和例 19.12 的方法以*差方法*著称. 例 19.15 表明同一思路的更复杂的应用.

现在我们知道，对 $v=13$，19，25，31，37，43，49，以及上面提到的值，存在$STS(v)$. 这包括了小于 50 的所有 $v\equiv1\pmod 6$. 事实上，我们现在知道对小于 100 的 $v$ 的可行值，除

234 了 $v=55$，$v=85$ 和 $v=91$，至少有一个 $STS(v)$.

**例 19.13** 设在点集 $V_i(i=1,2)$上有一个 $STS(v_i)$，我们取 $V_1\times V_2$ 作为一个新的点集且定义三元组$\{(x_1,y_1),(x_2,y_2),(x_3,y_3)\}$作为区组. 对于三元组$\{(x_1,y_1),(x_2,y_2),(x_3,y_3)\}$，

(1)$x_1=x_2=x_3$ 且$\{y_1,y_2,y_3\}$是 $STS(v_2)$的一个区组.

(2)$\{x_1,x_2,x_3\}$是 $STS(v_1)$的一个区组且 $y_1=y_2=y_3$.

(3)$\{x_1,x_2,x_3\}$是 $STS(v_1)$的一个区组且$\{y_1,y_2,y_3\}$是 $STS(v_2)$的一个区组.

很显然，这定义了一个 $STS(v_1v_2)$. 读者应检验我们已定义了区组的正确数目.

这一构造为我们提供了一个 $STS(91)$.

**例 19.14** 下面展示一个稍复杂些的构造. 假定我们有点集 $V_1=\{1,2,\cdots,v_1\}$上区组集为 $S_1$ 的 $STS(v_1)$，此外再假定完全包含在 $V=\{s+1,\cdots,v_1\}$中的区组构成一个 $STS(v)$，这

里 $s=v_1-v$. 设 $S_2$ 为点集 $V_2=\{1, 2, \cdots, v_2\}$ 上的 $STS(v_2)$ 的三元组的集合.

考虑新的点集

$$\mathcal{P}:=V\cup\{(x,y):1\leqslant x\leqslant s,1\leqslant y\leqslant v_2\}.$$

这个集合有 $v+v_2(v_1-v)$ 个点. 引入以下四种类型区组的一个集合 $\mathcal{B}$:

(1)子系统 $STS(v)$ 的那些区组.

(2)$\{(a, y), (b, y), c\}$, 满足 $c\in V$, $\{a, b, c\}\in S_1$ 且 $y\in V_2$.

(3)$\{(a, y), (b, y), (c, y)\}$, 满足 $\{a, b, c\}$ 是 $S_1$ 中的一个区组且没有一个点在 $V$ 中, 以及 $y\in V_2$.

(4)$\{(x_1, y_1)(x_2, y_2), (x_3, y_3)\}$, 其中 $\{y_1, y_2, y_3\}$ 是 $S_2$ 中的一个区组且整数 $x_1$, $x_2$, $x_3$ 满足

$$x_1+x_2+x_3\equiv 0(\mathrm{mod}\ s).$$

容易验证 $\mathcal{P}$ 中的两个点唯一地确定 $\mathcal{B}$ 中的一个区组. 因此, $\mathcal{P}$ 和 $\mathcal{B}$ 是 $v+v_2(v_1-v)$ 个点上的一个施泰纳三元系的点和区组. 设子系统恰为一个区组, 即 $v=3$, 得到一个简单的例子. 取 $v_1=7, v_2=13$, 可以找到 $STS(55)$.

于是, 对小于 100 的 $v$ 的每个可行的值, 除了 $v=85$, 我们已构造了 $STS(v)$. 235

**问题 19N** (a)证明: 如果 $STS(v_1)$ 和 $STS(v_2)$ 都存在, 则 $STS(v_1v_2-v_2+1)$ 存在. 利用这一构造寻找 $STS(85)$.

(b)在集合 $\{0, 1, \cdots, 14\}$ 上构造 $STS(15)$, 使得它包含 $\{0, 1, \cdots, 6\}$ 上的一个费诺平面作为子系统.

**例 19.15** 考虑点集 $\mathbb{Z}_{2t}\times\mathbb{Z}_3\cup\{\infty\}$. 元素的加法是带额外约定 $\infty+(x, i)=\infty$ 的按坐标相加. 为记号上方便起见, 有时我们把第二个坐标写成下标, 即用 $x_i$ 代替 $(x, i)$. 下面定义四种类型的"基区组":

(1)$\{0_0, 0_1, 0_2\}$.

(2)$\{\infty, 0_0, t_1\}$, $\{\infty, 0_1, t_2\}$, $\{\infty, 0_2, t_0\}$.

(3)$\{0_0, i_1, (-i)_1\}$, $\{0_1, i_2, (-i)_2\}$, $\{0_2, i_0, (-i)_0\}$, $i=1, \cdots, t-1$.

(4)$\{t_0, i_1, (1-i)_1\}$, $\{t_1, i_2, (1-i)_2\}$, $\{t_2, i_0, (1-i)_0\}$, $i=1, \cdots, t$.

我们有 $6t+1$ 个基区组. 对 $a=0, 1, \cdots, t-1$, 把元素 $(a, 0)$(即 $a_0$)加到每个基区组中的元素上, 于是产生 $t(6t+1)$ 个区组. 我们断言这些区组是 $STS(6t+1)$ 的三元组. 容易得到类型 2 的基区组产生一个区组集, 区组的每一对点中有一个是 $\infty$, 这样的点对恰出现一次. 基区组定义的循环性质表明, 对我们来说验证 $a\neq b$ 的所有对 $(a_0, b_0)$ 和出现在我们定义的三元组中的所有对 $(a_0, b_1)$ 就够了. 如果 $a<b$ 且 $b-a=2s$, 则从 $\{0_2, s_0, (-s)_0\}$ 得到的出现在三元组中的对 $\{a_0, b_0\}$ 由元素 $(b-s, 0)$"平移"而得到. 类似地, 如果 $b-a$ 是奇数, 我们通过平移类型 4 的一个基区组来寻找需要的对. 现在考虑对 $\{a_0, b_1\}$. 如果 $a=b\leqslant t-1$, 由 $(a, 0)$ 通过平移类型 1 的基区组寻找所要的对. 如果 $a\neq b$ 且 $a<t$, 我们必须通过平移类型 2 或类型 3 的基区组寻找所要的对. 我们一定要搜索一个基区组, 其中对两个元素 $y_1$, $x_0$ 差 $b-a$ 作为 $y-x$ 出

现. 对类型 2，这个差是 $t$，且在区组$\{0_0,\ i_1,\ (-i)_1\}$中找到满足 $1\leqslant i\leqslant t-1$ 的差 $i$，以及满足 $1\leqslant i\leqslant t-1$ 的差 $-i=2t-i$，事实上每个差出现一次！其余的细节留给读者作为练习.

这个例子表明，如果 $v=6t+1$，则存在一个 $STS(v)$. 结合例 19.11，我们已对每个可行 [236] 的 $v$ 有一个构造.

我们以费诺平面的一个有趣应用结束本章. 目前这个想法还没有在实际中应用，但问题自身有实际来源，而且也许有一天会用到下面方法的推广. 假设人们希望把整数 1 到 7 中的一个存储到所谓的"一次写入内存"中. 这是一种二进制内存，原来由零填充，可以把特定的比特变成 1，但不能再改回来，即状态 1 是永久的. 在实际中，这种情况应用于纸带时纸上被穿孔，应用于激光唱片时激光在唱片上特定的位置产生小坑. 在这两种情形，我们不能擦掉已写入的内存. 为了存储 1 到 7 的整数，我们需要 3 比特的内存. 如果人们希望接连四次使用内存会怎样？最简单的解法是有 12 比特的内存，它被划分为 3 比特的片断，每次接连使用一个片段. 假定内存非常昂贵，我们希望能用较小的内存达到同样的目的. 下面我们证明 7 比特就够了，节约超过 40%.

设$\mathcal{P}=\{1,\ 2,\ \cdots,\ 7\}$是 $PG_2(2)$的点集，又设$\mathcal{L}$表示线的集合. 为了在内存中存储 1 到 7 的整数，对内存中的位置从 1 到 7 编号，我们使用如下普遍的规则：如果希望存储 $i$，而这个内存处于对应 $i$ 的状态(由前一次使用得来)，那么什么也不做. 否则，规则为：

(1)如果内存是空的，通过在位置 $i$ 置 1 存储 $i$.

(2)当内存处于状态 $i$ 时，为存储 $j$，在位置 $k$ 置 1，这里$\{i,\ j,\ k\}\in\mathcal{L}$.

(3)当内存中包含两个 1 但不与 $i$ 对应时，为存储 $i$，再置两个 1，使得 $i$ 是四个 1 中的一 [237] 个，且另外的三个 1 在$\mathcal{L}$的一条线上. 无论原来的两个 1 的位置怎样，这是可能的(有时有两种方式).

(4)如果内存中有四个 1，可以假设我们处在图 19.3 所示的情形. 为存储 3，我们什么也不用做(由普遍的规则)；为存储缺失的数，在其余的两个位置上置 1；为存储 1，2 或者 4，在穿过 3 和要存储的那个数的线的空位置上置 1.

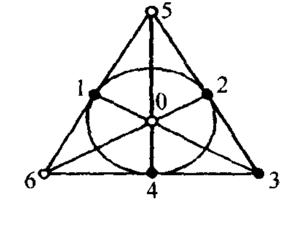


图　19.3

我们把列出读取内存的规则作为练习留给读者. 注意，内存唯一地读取当前存储在该内存中的整数，但是不能看到一个整数所存储的次数或者上一次存储的是哪个整数.

**问题 19O**　(i)假设$\mathcal{A}$是一个 $n$-集合 $X$ 的子集族，使得$\mathcal{A}$的任何一个成员的基数是奇数，又使得$\mathcal{A}$的任意两个成员交于偶数个点. 证明 $|\mathcal{A}|\leqslant n$.

(ii)假设$\mathcal{A}$的成员的基数是偶数且任意两个成员交于奇数个点. 证明 $|\mathcal{A}|\leqslant n+1$. 你能找到等号成立的例子吗？

**问题 19P**　考虑 2-$(v,\ k,\ \lambda=2)$设计，这里 $v=\binom{k+1}{2}$.

(i)找出 $k=3$ 的一个例子.（你可以尝试五个点在圆周上且一个点在中央.）

(ii)设 $A_1,\ A_2,\ \cdots,\ A_b$ 是区组且对 $i=2,\ 3,\ \cdots,\ b$，设 $\mu_i=|A_i\cap A_1|$. 根据 $k$ 计算

$$\sum_{i=2}^{b}\mu_i,\quad \sum_{i=2}^{b}\mu_i(\mu_i-1),\quad \sum_{i=2}^{b}(\mu_i-1)(\mu_i-2).$$

关于 $\mu_i$ 你有何解释?

**问题 19Q** 广义施泰纳系是一个关联结构，它有规模为 $v$ 的一个点集$\mathcal{P}$以及$\mathcal{P}$的子集的一个集合$\mathcal{B}$，仍称为区组，这里 $|\mathcal{B}|=b$，使得$\mathcal{P}$的每个 $t$-子集在唯一一个区组中. 我们不要求区组有相同的规模但排除 $b=1$ 的平凡情形. 用 $b_{t,v}$表示一个非平凡的广义施泰纳系的最小值$b$. 证明对 $t\geqslant 2$，有 [238]

$$b_{t,v}(b_{t,v}-1)\geqslant t\binom{v}{t}.$$

注意对 $t=2$，这个结果与定理 19.1 相同. 强得多的界是已知的但不易导出.

**问题 19R** 我们说费诺平面上的一个点是一条线的代表，如果它与这条线关联. 费诺平面有多少 SDR?

**问题 19S** 对所有的 $k\geqslant 2$，构造 3-$(2^k,4,1)$设计.

**问题 19T** 我们说一个设计能被扩展，如果它是扩展设计所导出的设计. 证明：如果一个对称设计能被扩展两次，则它一定是 2-(21，5，1)设计.

**问题 19U** 考虑问题 1J 中的图 $G$. 以 $G$ 的顶点作为点且对顶点 $x\in G$，集合 $\Gamma(x)$作为线定义一个关联结构 $\boldsymbol{I}$. 证明 $G$ 的性质蕴涵 $\boldsymbol{I}$ 是一个射影平面.（参见问题 21Q.）

**问题 19V** 我们利用定理 19.8 的假设，以及在定理 19.8 的证明中引入的记号.

(i)验证 $W_{is}N_s=\binom{k-i}{s-i}N_i$.

(ii)对 $i=0,1,\cdots,s$，证明 $W_{is}^{\top}W_{is}$中任意两个的乘积是 $s+1$ 个这样的矩阵的线性组合. 因此这些矩阵的线性生成$\mathcal{A}$对乘法封闭.

(iii)假定在定理 19.8 中等号成立，因此矩阵 $N_s$ 是一个方阵. 那么 $N_s^{\top}M^{-1}N_s=I$，这里 $M:=\sum_{i=0}^{s}b_{2s-i}^{i}W_{is}^{\top}W_{is}$. 因为 $M\in\mathcal{A}$，(ii)蕴涵 $M^{-1}\in\mathcal{A}$. 由此证明存在一个次数为 $s$ 的多项式 $f(x)$，对所有不同的区组 $A$，$B$ 使得 $f(|A\cap B|)=0$.（因此至多有 $s$ 个“相交数”.）这个结果推广了定理 19.9.

## 评注

第一次出现的 2-设计可能是 Plücker(1839)的一篇论文中的 $AG_2(3)$. 人们通常把施泰纳系的引入归功于 Woolhouse(1844)，当然没有归功于施泰纳！施泰纳系常常被说成源于 T. P. Kirkman(1847)的一个问题. T. P. Kirkman(1806—1895)自学成材，是英国基督教会的牧师. 他是一位业余数学家，对设计这一分支有许多贡献. 最著名的可能是他的 15 个女生问题. 这个问题是把 15 个女生分成三组，在七天的散步中她们中的每两个人恰在一起一次. 这相当于构造一个 $STS(15)$，对于它三元组能被划分成七个“平行类”. [239]

施泰纳(Jakob Steiner，1796—1863)是他所在时代的一个重要的几何学家. 在 1853 年，当他研究一条平面四次曲线的 28 条二重切线时对现在所说的施泰纳系产生了兴趣.

费希尔(Ronald A. Fisher, 1890—1962)爵士被认为是最杰出的统计学家之一. 除对统计学(多变量分析)和遗传学的重要贡献之外, 他还以统计理论对农业和实验设计的应用而著名. 把统计应用到农业实验的设计解释了 $v$ 和 $r$ 的使用, 即用 $v$ 表示设计中点的数目(varieties), 用 $r$ 表示穿过一点的区组的数目(replication number).

定理 19.7 属于 M. P. Schutzenberger(1949).

费希尔不是对设计的数学理论做出贡献的唯一统计学家. 事实上, 我们可能应该认为印度数学家 R. C. Bose(1901—1987)是其中最重要的一位. 本章描述的构造方法中, 很多(如差法)属于他.

费诺(G. Fano, 1871—1952)的名字与平面 $PG_2(2)$相连, 他在意大利射影几何学派中是重要的一员.

有限域上的射影平面最先由 K. G. C. von Staudt(1798—1867)在他的书《Geometrie der Lage》(1856)中加以研究.

不可嵌入的拟剩余设计的第一个例子由 Bhattacharya(1944)给出. 它也是 2-(16, 6, 3)设计. 然而, 例 19.9 是一个简单得多的例子.

240 拉格朗日(J. L. Lagrange, 1736—1813)在意大利出生并接受教育, 但他被认为是法国数学家(他在柏林做研究). 除对分析的许多贡献之外, 他还以数论中的几个定理而著名.

Bruck-Ryser-Chowla 定理(即定理 19.11)是众所众知的, 通常称为 BRC.

例 19.15 的想法属于 Skolem(1958). 实际上他的想法有些不同. 它导致了术语斯科伦(Skolem)序列. 这些序列有其他应用, 如在射电天文学中. 他的想法如下: 集合$\{1, 2, \cdots, 2n\}$划分成$\{a_i, b_i\}$使得 $b_i - a_i = i$, $1 \leqslant i \leqslant n$. 这是一个斯科伦序列. 例如, $\{9, 10\}$, $\{2, 4\}$, $\{5, 8\}$, $\{3, 7\}$, $\{1, 6\}$是对 $n=5$ 的划分. 现在形成三元组$\{0, a_i+n, b_i+n\}$并且把它们作为基区组(mod $6n+1$). 因为所有的差 $1, 2, \cdots, 3n$ 和它们的相反数恰出现一次, 所以这些区组构成一个 $STS(6n+1)$.

戈莱码(参见第 20 章)对一次写入内存的一个有趣的应用, 见 Cohen et al(1986). 他们证明在 23 个位置上能三次接连写入 11 比特.

## 参考文献

W. O. Alltop (1972), An infinite class of 5-designs, *J. Combinatorial Theory* (A) **12**, 390–395.

K. N. Bhattacharya (1944), A new balanced incomplete block design, *Science and Culture* **9**, 108.

R. H. Bruck and H. J. Ryser (1949), The non-existence of certain finite projective planes, *Canad. J. Math.* **1**, 88–93.

N. G. de Bruijn and P. Erdős (1948), On a combinatorial problem, *Proc. Kon. Ned. Akad. v. Wetensch.* **51**, 1277–1279.

K. Chandrasekharan (1968), *Introduction to Analytic Number Theory*, Springer-Verlag.

S. Chowla and H. J. Ryser (1950), Combinatorial problems, *Canad. J. Math.* **2**, 93–99.

G. D. Cohen, P. Godlewski, and F. Merkx (1986), Linear binary codes for write-once memories, *IEEE Trans. Information Theory* **32**, 697–700.

W. S. Connor, Jr. (1952), On the structure of balanced incomplete block designs, *Ann. Math. Stat.* bf 23, 57–71; correction *ibid.* **24**, 135.

[241]

R. H. F. Denniston (1976), Some new 5-designs, *Bull. London Math. Soc.* **8**, 263–267.

G. Fano (1892), *Giornale di Matimatiche* **30**, 114–124.

M. J. Granell and T. S. Griggs (1994), A Steiner system $S(5,6,108)$, *Discrete Mathematics* **125**, 183–186.

D. Jungnickel and S. A. Vanstone (1987), Hyperfactorizations of graphs and 5-designs, *J. Univ. Kuwait (Sci)* **14**, 213–223.

T. P. Kirkman (1847), On a problem in combinations, *Cambridge and Dublin Math. J.* **2**, 191–204.

D. L. Kreher and S. P. Radziszowski (1986), The existence of simple 6-(14,7,4) designs, *J. Combinatorial Theory* (A) **41**, 237–243.

C. W. Lam, S. Swiercz, and L. Thiel (1989), The nonexistence of finite projective planes of order 10, *Canad. J. Math.* **41**, 1117–1123.

D. W. Leavitt and S. S. Magliveras (1982), Simple 6-(33,8,36)-designs from $P\Gamma L_2(32)$, pp. 337–352, in: *Computational Group Theory, Proc. Durham* 1982.

W. H. Mills (1978), A new 5-design, *Ars Combinatoria* **6**, 193–195.

A. Ya. Petrenjuk (1968), On Fisher's inequality for tactical configurations (in Russian), *Mat. Zametki* **4**, 417–425.

D. K. Ray-Chaudhuri and R. M. Wilson (1975), On $t$-designs, *Osaka J. Math.* **12**, 737–744.

H. J. Ryser (1963), *Combinatorial Mathematics*, Carus Math. Monograph **14**.

M. P. Schutzenberger (1949), A non-existence theorem for an infinite family of symmetrical block designs, *Ann. Eugenics* **14**, 286–287.

Th. Skolem (1958), Some remarks on the triple systems of Steiner, *Math. Scand.* **6**, 273–280.

J. Steiner (1853), Combinatorische Aufgabe, *J. f. d. reine u. angew. Mathematik* **45**, 181–182.

L. Teirlinck (1987), Nontrivial $t$-designs without repeated blocks exist for all $t$, *Discrete Math.* **65**, 301–311.

J. Tits (1964), Sur les systèmes de Steiner associés aux trois 'grands' groupes de Mathieu, *Rend. Math. e Appl.* (5) **23**, 166–184.

E. Witt (1938), Die 5-fach transitiven Gruppen von Mathieu, *Abh. Math. Sem. Univ. Hamburg* **12**, 256–264.

[242]

W. S. B. Woolhouse (1844), Prize question 1733, *Lady's and Gentleman's Diary.*

[243]

# 第20章 码和设计

我们从纠错码理论引入更多的术语. 在最普遍的意义上，长度为 $n$ 的码就是一个子集 $C\subseteq S^n$，这里 $S$ 是有限集(字母表). $C$ 的元素称为码字. 二元码是字母表 $S=\{0, 1\}$的码，三元码是 $S=\{0, 1, 2\}$的码. 在 $S^n$ 中两个字(向量)$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 之间的距离 $d(\boldsymbol{x}, \boldsymbol{y})$定义为位置的数目，它们在那些位置上不相同，即

$$d(\boldsymbol{x},\boldsymbol{y}) := |\{i : 1 \leqslant i \leqslant n, x_i \neq y_i\}|. \tag{20.1}$$

这其实是通常意义下的距离函数；验证它满足三角不等式.

距离的概念导致几何术语的应用，例如，集合 $B_r(\boldsymbol{x}) := \{\boldsymbol{y}\in \mathbb{F}_q^n : d(\boldsymbol{x}, \boldsymbol{y})\leqslant r\}$称为半径为 $r$ 且中心为 $\boldsymbol{x}$ 的球.

码 $C$ 的最小距离 $d$ 是

$$d := \min\{d(\boldsymbol{x},\boldsymbol{y}) : \boldsymbol{x} \in C, \boldsymbol{y} \in C, \boldsymbol{x} \neq \boldsymbol{y}\}. \tag{20.2}$$

编码论中的许多内容与线性码有关. $q$ 元$[n, k]$码是指向量空间$\mathbb{F}_q^n$的 $k$ 维线性子空间 $C$.

$\boldsymbol{x}$ 的重量 $w(\boldsymbol{x})$由

$$w(\boldsymbol{x}) := d(\boldsymbol{x},\boldsymbol{0}) \tag{20.3}$$

244

定义. 只要 0 是符号(字母表的元素)之一就可以定义重量，但尤其对线性码有意义. 若 $C$ 是线性的，两个码字 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 之间的距离等于 $\boldsymbol{x}-\boldsymbol{y}$ 的重量，$\boldsymbol{x}-\boldsymbol{y}$ 是另一个码字. 于是 $C$ 的最小距离等于最小重量，即非零码字的最小重量. 我们用记号$[n, k, d]$码表示最小距离至少为 $d$ 的$[n, k]$码. 如果 $d=2e+1$，则称 $C$ 为 $e$-纠错码.

码 $C$ 的覆盖半径$\rho(C)$定义为最小的 $R$，使得半径为 $R$ 且码字作为中心的球覆盖 $S^n$，即

$$\rho(C) := \max\{\min\{d(\boldsymbol{x},\boldsymbol{c}) : \boldsymbol{c} \in C\} : \boldsymbol{x} \in S^n\}. \tag{20.4}$$

在第 18 章，我们曾提到$\{0, 1\}^n$ 中的重复码，即仅包含 $\boldsymbol{0}$ 和 $\boldsymbol{1}$ 的$\mathbb{F}_2^n$的一维子空间. 如果 $n=2e+1$，则一个字恰到一个码字有$\leqslant e$ 的距离. 因此，这个码的覆盖半径为 $e$. 半径为 $e$ 的两个球围绕两个码字，它们不相交且覆盖空间$\mathbb{F}_2^n$.

一般来说，我们称不必是线性码的码 $C\subseteq S^n$ 为($e$-纠错)完全码，如果 $|C|>1$ 且任意一个 $x\in S^n$ 恰好到一个码字有$\leqslant e$ 的距离. 这等价于 $C$ 有最小距离 $d=2e+1$ 和覆盖半径 $e$. 显然，完全码是组合学中的有趣对象. 然而它们极为罕见.

**定理 20.1** 如果在 $S^n$ 中 $C$ 是距离 $d\geqslant 2e+1$ 的码，则

$$|C|\cdot \sum_{i=0}^{e}\binom{n}{i}(q-1)^i \leqslant q^n. \tag{20.5}$$

**证明** (20.5)左端的和对半径为 $e$ 的球中的字的数目进行计数. ■

这个定理中的界以球装填界或汉明界著称. 如果等号成立，则 $C$ 是完全码.

245

**问题 20A** 证明：如果[23, 12, 7]二元码存在，则这个码是完全的.

**问题 20B** 由(20.5)，长度为 6 且最小距离为 3 的二元码至多有 9 个码字. 证明等号不成立(然而，8 是可能的).

两个码称为等价的，如果通过 $S^n$ 中坐标位置的某个排列能从一个码得到另一个码. 有时通过允许 $S$ 的元素的排列，例如，$S=\mathbb{F}_3$时，$+1$ 和 $-1$ 交换，可以扩展这个定义.

$k\times n$ 矩阵 $G$ 称为$[n, k]$码 $C$ 的生成矩阵，如果 $C$ 由 $G$ 的行张成. 初等线性代数证明 $C$ 等价于生成矩阵为$G=[I_k \quad P]$的一个码，这里 $P$ 是某个 $k\times(n-k)$矩阵. 这称为生成矩阵的约化阶梯形.

$C$ 的对偶 $C^{\perp}$ 由

$$C^{\perp} := \{x \in \mathbb{F}_q^n : \forall_{c\in C}\langle x, c\rangle = 0\} \tag{20.6}$$

定义. 如果 $H$ 是 $C^{\perp}$ 的生成矩阵，则显然

$$C = \{x \in \mathbb{F}_q^n : xH^{\top} = \mathbf{0}\}. \tag{20.7}$$

$H$ 称为码 $C$ 的奇偶校验矩阵. 如果 $G=[I_k \quad P]$是一个生成矩阵，则 $H=[-P^{\top} \quad I_{n-k}]$是一个奇偶校验矩阵. 如果 $C=C^{\perp}$，称 $C$ 为自对偶码. 如果 $C\subseteq C^{\perp}$，则称 $C$ 是自正交的.

如果 $C$ 是$\mathbb{F}_q^n$中的一个线性码，则扩展码 $\bar{C}$ 由

$$\bar{C} := \{(c_1, \cdots, c_n, c_{n+1}) : (c_1, \cdots, c_n) \in C, c_1 + \cdots + c_{n+1} = 0\} \tag{20.8}$$

定义. 符号 $c_{n+1}$称为奇偶校验符.

**例 20.1** 设 $n=(q^k-1)/(q-1)$. 考虑项在$\mathbb{F}_q$ 中的规模为$k\times n$ 的矩阵 $H$，其中的列是两两线性无关的. 注意，这是对 $H$ 可能的 $n$ 的最大值. 显然，$H$ 是最小距离为 3 的$[n, n-k]$码的奇偶校验矩阵. 这样的码称为 $q$ 元汉明码. 如果 $\boldsymbol{c}$ 是一个码字，则 $|B_1(\boldsymbol{c})|=1+n(q-1)=q^k$. 因为 $|C|=q^{n-k}$，由(20.5)我们得知这个码是完全的. 246

**问题 20C** 设 $H$ 为三元$[4, 2]$汉明码. 由码字

$$(x_0, x_1, \cdots, x_4; y_1, \cdots, y_4)$$

定义一个长度为 9 的(非线性)三元码 $C$，要求 $\sum_{i=0}^{4} x_i\neq 0$ 且$(y_1-x_1, \cdots, y_4-x_4)$是 $H$ 中的一个码字. 证明 $C$ 的覆盖半径为 1.（现在尚不知道长度为 9、覆盖半径为 1 且码字少于 $2\cdot 3^6$ 的三元码.）

**例 20.2** 考虑长度 $n=2^k-1$ 的二元汉明码 $C$. 由定义，它的对偶码 $C^{\perp}$的生成矩阵是长度为 $k$ 的所有可能的非零向量作为列的 $k\times n$ 矩阵. 所以，$C^{\perp}$ 的扩展是第 18 章的码 $R'(1, k)$. $C^{\perp}$ 通常称为长度为 $n$ 的单纯形码. 注意，$[8, 4]$扩展二元汉明码是自对偶的.

**问题 20D** 证明码 $R(1, 2k)$的覆盖半径是 $2^{2k-1}-2^{k-1}$.（提示：用$\pm 1$ 表示代替$(0, 1)$，在$\mathbb{Q}$上证明覆盖半径至多有这么大. 考虑字 $\boldsymbol{z}$，它是

$$\{x \in \mathbb{F}_2^{2k} : x_1x_2 + \cdots + x_{2k-1}x_{2k} = 1\}$$

的特征函数，证明相等性.）

我们提及对任意码容易证明的界，即 Singleton 界.

**定理 20.2** 设 $C$ 是$\mathbb{F}_q$ 上长度为 $n$ 且最小距离为 $d$ 的任意码. 则

$$|C| \leqslant q^{n-d+1}.$$

**证明** 从每个码字，我们删去最后的 $d-1$ 个符号. “缩短的”字的集合由两两不同的字构成！它们不超过 $q^{n-d+1}$. ■ 247

**例 20.3** 我们给出与第 19 章有良好联系的一个例子. 设 $q=2^a$. $S$ 是 $PG_2(q)$中的超卵形. 利用例 19.7 中的术语，$S$ 的元素是$\mathbb{F}_q^3$中的向量，它们满足没有三个向量是线性相关的性质. 我们取 $S$ 的元素作为 $3\times(q+2)$矩阵 $H$ 的列. 如果把 $H$ 解释成$\mathbb{F}_q$ 上$[q+2, q-1]$码的奇偶校验矩阵，则这个码的最小距离至少为 4. 于是由定理 20.2，这个距离等于 4. 这是定理 20.2 中等号成立的罕见的例子之一. 使 Singleton 界等号成立的码称为最大距离可分离码(MDS 码)，这又是一个不幸的名字！关于这些码有许多未解决的问题.

如果 $C$ 是一个 $q$ 元$[n, k]$码，且 $A_i$ 表示 $C$ 中重量为 $i$ 的码字的数目，则

$$A(z) := \sum_{i=0}^{n} A_i z^i \tag{20.9}$$

称为 $C$ 的重量计数器. 当然，$A_0=1$ 且 $A(1)=|C|=q^k$.

**问题 20E** 设 $C$ 是一个二元码，不必是线性的，码的长度为 23，最小距离为 7 且 $|C|=2^{12}$. 假定 $\mathbf{0}\in C$. 首先证明 $C$ 是完全码. 设 $C$ 的重量计数器由(20.9)给出. $\boldsymbol{c}\in C$，$w(\boldsymbol{x})=4$ 且 $d(\boldsymbol{x}, \boldsymbol{c})=3$,计算对子$(\boldsymbol{x}, \boldsymbol{c})$的个数并证明 $A_7=253$. 然后证明 $C$ 的重量计数器事实上由 $C$ 是完全码和 $\mathbf{0}\in C$ 完全确定.

下面的定理是纠错码理论中最有用的定理之一. 它属于 F. J. MacWilliams(1963).

**定理 20.3** 设 $C$ 是$\mathbb{F}_q$ 上重量计数器为 $A(z)$的$[n, k]$码，又设 $B(z)$为 $C^\perp$ 的重量计数器，则

$$B(z) = q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right). \tag{20.10}$$

**证明** 我们仅给出 $q=2$ 时的证明. 对 $q$ 的其他值，证明在本质上是一样的(一定要用 $\chi(\langle \boldsymbol{u}, \boldsymbol{v}\rangle)$代替下面所用的$(-1)^{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}$，这里 $\chi$ 是$\mathbb{F}_q$ 上的一个特征).

248

定义

$$g(\boldsymbol{u}) := \sum_{\boldsymbol{v}\in \mathbb{F}_2^n} (-1)^{\langle \boldsymbol{u}, \boldsymbol{v}\rangle} z^{w(\boldsymbol{v})}.$$

则

$$\sum_{\boldsymbol{u}\in C} g(\boldsymbol{u}) = \sum_{\boldsymbol{u}\in C}\sum_{\boldsymbol{v}\in \mathbb{F}_2^n} (-1)^{\langle \boldsymbol{u}, \boldsymbol{v}\rangle} z^{w(\boldsymbol{v})} = \sum_{\boldsymbol{v}\in \mathbb{F}_2^n} z^{w(\boldsymbol{v})} \sum_{\boldsymbol{u}\in C} (-1)^{\langle \boldsymbol{u}, \boldsymbol{v}\rangle}.$$

这里，如果$\boldsymbol{v}\in C^\perp$，则内和是$|C|$；如果$\boldsymbol{v}\notin C^\perp$，则内和中一半的项的值为+1，另一半为-1. 因此

$$\sum_{\boldsymbol{u}\in C} g(\boldsymbol{u}) = |C|\cdot B(z). \tag{20.11}$$

现在

$$\begin{aligned} g(\boldsymbol{u}) &= \sum_{(v_1, v_2, \cdots, v_n)\in \mathbb{F}_2^n} \prod_{i=1}^{n} ((-1)^{u_i v_i} z^{v_i}) \\ &= \prod_{i=1}^{n} (1+(-1)^{u_i} z) \\ &= (1-z)^{w(\boldsymbol{u})}(1+z)^{n-w(\boldsymbol{u})}. \end{aligned}$$

在(20.11)中代入 $g(\boldsymbol{u})$得到定理的结果. ■

**推论** 如果把 $B(z)$写成 $B(z)=\sum_{j=0}^{n}B_j z^j$，则对 $q=2$，从(20.10)中可以发现

$$B_j = 2^{-k}\sum_{i=0}^{n}A_i\sum_{l=0}^{j}(-1)^l\binom{i}{l}\binom{n-i}{j-l}. \tag{20.12}$$

这些关系称为 MacWilliams 关系，给定系数 $B_j$，它们是系数 $A_i$ 的线性无关方程.

许多已知的非平凡 5-设计由下面 MacWilliams 定理的优美应用而得到，通常把得到的这些结果称为 Assmus-Mattson 定理(1969). 我们再次把证明限制在二元情形. 对其余的 $q$，用差不多相同的证明，得到该定理显而易见的推广. 把长度为 $n$ 的码的位置与集合 $\mathcal{P}:=\{1, 2, \cdots, n\}$等同起来. 这允许我们把二元码中的一个码字解释为$\mathcal{P}$的一个子集(即作为一个子集的特征函数). 码字的支撑是该码字不为零的坐标位置的集合. [249]

**问题 20F** 设 $C$ 是长度为 $n$ 的完全二元 $e$-纠错码. 假定 0 是符号且 $\mathbf{0}$ 是码字. 证明$\mathcal{P}$与重量 $d=2e+1$ 的码字的支撑合在一起是 $S(e+1, 2e+1, n)$.

**定理 20.4** *设 $A$ 是一个二元$[n, k, d]$码，又设 $B:=A^{\perp}$是它的对偶码，即$[n, n-k]$码. 设 $t<d$. 假设 $B$ 中小于或等于 $n-t$ 的非零重量的数目$\leqslant d-t$. 则对每个重量 $w$，$A$ 中重量为 $w$ 的字的支撑构成一个 $t$-设计，且 $B$ 中重量为 $w$ 的字的支撑构成一个 $t$-设计.*

**证明** 如果 $C$ 是任意码且$\mathcal{P}$的一个 $t$-子集 $T$ 固定，则用 $C'$表示从 $C$ 中的码字删掉 $T$ 中的坐标得到的长度为 $n-t$ 的码. 再用 $C_0$ 表示从 $T$ 的所有位置上为零的 $C$ 中的码字删去 $T$ 中的坐标得到的 $C'$的子码.

证明分四步.

(i)设 $T$ 是规模为 $t$ 的$\mathcal{P}$的子集. 因为 $t$ 小于 $A$ 的最小距离，码 $A'$与 $A$ 有同样多的码字，即也有维数 $k$. 事实上，$A'$仍有$\geqslant d-t$ 的最小距离. 于是对偶$(A')^{\perp}$有维数 $n-k-t$. 显然，$B_0$ 是$(A')^{\perp}$的一个子码. 因为 $B_0$ 的维数至少为 $n-k-t$，因此一定有 $B_0=(A')^{\perp}$.

(ii)设$\sum\alpha_i z^i$ 和$\sum\beta_i z^i$ 分别是 $A'$和 $B_0$ 的重量计数器. 我们断言这些重量计数器不依赖特定的 $t$-子集 $T$，而仅依赖数 $t$，$n$，$k$，以及 $B$ 中字的重量.

设 $0<\ell_1<\ell_2<\cdots<\ell_r\leqslant n-t$ 是码 $B$ 的$\leqslant n-t$ 的非零重量，这里 $r\leqslant d-t$. 这是 $B_0$ 仅有的可能的重量. 则(20.12)给出 [250]

$$|B_0|\alpha_j = \binom{n-t}{j}+\sum_{i=1}^{r}\beta_{\ell_i}\sum_{m=0}^{j}(-1)^m\binom{\ell_i}{m}\binom{n-t-\ell_i}{j-m}.$$

由假设，$A'$的最小距离$\geqslant r$，于是我们知道 $j<r$ 时 $\alpha_j$ 的值，即 $\alpha_0=1$，$\alpha_1=\cdots=\alpha_{r-1}=0$. 因此我们有 $r$ 个未知量$\beta_{\ell_i}$的 $r$ 个线性方程. 如果 $r\times r$ 系数矩阵 $M$ 是非奇异的，这些未知量被唯一地确定，$M$ 的$(i, j)$项为 $p_j(\ell_i)$，其中

$$p_j(x):=\sum_{m=0}^{j}(-1)^m\binom{x}{m}\binom{n-t-x}{j-m},$$

$1\leqslant i\leqslant r$，$0\leqslant j\leqslant r-1$. 但 $p_j(x)$是次数恰好为 $j$ 的多项式($x^j$ 的系数是$(-1)^j 2^j/j!$)，通过初等

列运算，$M$ 化为范德蒙德(Vandermonde)矩阵

$$\begin{bmatrix} 1 & \ell_1 & \ell_1^2 & \cdots & \ell_1^{r-1} \\ 1 & \ell_2 & \ell_2^2 & \cdots & \ell_2^{r-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \ell_r & \ell_r^2 & \cdots & \ell_r^{r-1} \end{bmatrix},$$

因为 $\ell_i$ 互不相同，所以这个矩阵是非奇异的.

于是重量计数器 $\sum \beta_i z^i$ 不依赖子集 $T$ 的选择. 因为 $A'$ 是 $B_0$ 的对偶，所以 $\sum \alpha_i z^i$ 也不依赖 $T$.

(iii)设 $\mathcal{E}$ 为 $B$ 中重量为 $w$ 的字集，视为 $\mathcal{P}$ 的子集. 失去 $T$ 中所有坐标的 $\mathcal{E}$ 的成员数等于 $B_0$ 中重量为 $w$ 的成员数，这也不依赖 $T$. 也就是说，($\mathcal{P}$，$\mathcal{E}$)的补是一个 $t$-设计. 由问题 19C，$\mathcal{E}$ 中的集合构成 $t$-设计的区组. 这就证明了定理的第二个断言.（注意：如果 $w>n-t$，这种证法可能受到批评. 但在这种情形，当我们的论证用于 $t':=n-w$ 时，说明或者每个 $w$-子集是一个码字的支撑，或者没有 $w$-子集是码字的支撑；所以重量为 $w$ 的字，如果有的话，构成一个平凡的 $t$-设计.）

251

(iv)我们用归纳法证明定理的第一个断言. 从 $w=d$ 开始. 设 $\mathcal{D}$ 是 $A$ 中重量为 $d$ 的字集. $\mathcal{D}$ 中包含 $\mathcal{P}$ 的给定 $t$-子集 $T$ 的集合数等于 $A'$ 中重量为 $d-t$ 的字的数目，正如我们在上面所看到的，这个数字不依赖 $T$ 的选择. 于是 $\mathcal{D}$ 是一个 $t$-设计. 设 $w>d$ 并假设断言对所有的 $w'$ 成立，满足 $w \geqslant w' > d$. 现在设 $\mathcal{D}$ 表示 $A$ 中重量为 $w$ 的字集. 在这种情形，$\mathcal{D}$ 中包含给定的 $t$-子集 $T$ 的子集数等于 $A'$ 中与 $A$ 中重量为 $w$ 的码字对应的重量为 $w-t$ 的字的数目. 由(iii)，$A'$ 中重量为 $w-t$ 的字的总数不依赖 $T$ 的选择. 由归纳假设和(19.6)，$A'$ 中与 $A$ 中重量小于 $w$ 的码字对应的重量为 $w-t$ 的字的数目不依赖 $T$ 的选择. 这就证明了第一个断言. ■

**问题 20G** 长度为 $2^r-1$ 的二元汉明码的对偶的重量计数器是什么？导出这个汉明码自身的重量计数器的表达式.

**例 20.4** 设 $A$ 为扩展的[8，4]二元汉明码. 我们知道 $A=A^{\perp}$. 按照定理 20.4 的记号，我们有 $d=4$. 取 $t=3$. 定理 20.4 的条件得以满足. 因此重量为 4 的字构成一个 3-设计，这当然是对应于 $R(1,3)$的阿达马 3-(8，4，1)设计.

**例 20.5** 在下一个例子之后，我们将讨论著名的二元戈莱(Golay)码，并证明它对应的扩展码 $G_{24}$ 是具有重量 0，8，12，16 和 24 的自对偶[24，12，8]码. 于是定理 20.4 表明这个码中重量为 8 的字组成一个 5-设计. 由问题 20E，我们知道该设计有 759 个区组，(19.1)表明 $\lambda=1$. 这还可由该码有距离 8，因此两个区组至多有四个公共点得出. 这个设计是第 19 章提到的维特(Witt)设计 $S(5,8,24)$. 其他重量的字也产生 5-设计.

**例 20.6** 下面的 5-设计以及其他设计，是由 V. Pless(1972)发现的. 考虑由(18.5)给出的 $18\times 18$ Paley 矩阵 $C$. 我们考虑生成矩阵 $G=[I_{18} \quad C]$的一个三元[36，18]码 $Sym_{36}$. 这样的码称为对称码. 因为 $C$ 是 Paley 矩阵，我们有 $GG^{\top}=O$，即 $Sym_{36}$ 是一个自对偶码. 这蕴涵着在该码中所有的重量能被 3 整除. 我们断言 $Sym_{36}$ 中的字重量至少为 12. 因为 $C$ 是对称的，矩阵$[-C \quad I_{18}]$是该码的一个奇偶校验矩阵，又因为这个码是自对偶的，这意味着这个矩阵也是

252

该码的一个生成矩阵．如果$(\boldsymbol{a}, \boldsymbol{b})$是一个码字，这里$\boldsymbol{a}$和$\boldsymbol{b}$是$\mathbb{F}_3^{18}$中的向量，则$(-\boldsymbol{b}, \boldsymbol{a})$也是一个码字．这表明如果存在一个重量小于12的码字，则存在这样一个码字，它是$G$的至多四行的线性组合．这些容易用手算验证如下；读者应把它作为一个练习．$C$是一个Paley矩阵的事实和定理18.1的证明中(以及问题18B中)所用的论证表明，$G$的1，2或3行的线性组合分别有重量18，12，12或15．剩下需要验证四行的组合．现在利用(18.5)中$Q$是循环的这一事实，它蕴涵仅有几个本质上不同的组合需要验证．也可以通过一行扩大定理18.1的证明中所用的阵列．两种方法涉及很少的工作就能产生最小重量是12这一结果．(这最初是用计算机做的．)

我们现在把定理20.4的推广用于三元码．如果在$Sym_{36}$中考虑重量固定的字(定理的推广对重量12，15，18和21成立)，且把每个字用非零坐标出现的位置的集合代替，则得到5-设计．因为码字$\boldsymbol{c}$和$2\boldsymbol{c}$产生同一个集合，所以我们仅把这个集看成一个区组．

我们现在遇到所有二元码中最著名的码：*二元戈莱码* $G_{23}$．这个码有许多构造方法，其中一些很优雅且对码的性质有短的证明．我们仅展示这些构造中与设计理论相关的一个．

我们考虑(唯一的)2-(11，6，3)设计的关联矩阵$N$，见问题19D．我们有$NN^{\top}=3I+3J$．把$N$看成项在$\mathbb{F}_2$中的一个矩阵，则$NN^{\top}=I+J$．于是$N$的秩为10且使$\boldsymbol{x}N=\boldsymbol{0}$的唯一向量$\boldsymbol{x}$是$\boldsymbol{1}$．这一设计的性质显然蕴涵任意一行的重量为6且$N$的两行之和的重量为6．我们还知道$N$的三行或四行的和不是$\boldsymbol{0}$．

253

接下来，设$G=(I_{12}\ P)$是$\mathbb{F}_2$上的$12\times 24$矩阵，这里

$$P=\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & N & \\ 1 & & & \end{bmatrix}. \tag{20.13}$$

$G$的每一行的重量$\equiv 0 \pmod 4$，任意两行的内积为0．这蕴涵着$G$的行的任意线性组合的重量$\equiv 0 \pmod 4$；这可由归纳法证明．关于$N$做的观察此后显示$G$的行的任意线性组合的重量至少为8．考虑由$G$生成的码并称之为$G_{24}$．删除任一坐标以得到最小距离至少为7的一个二元$[23, 12]$码．由问题20A，这个码的最小距离一定等于7，此外它是一个*完全码*！我们把它记为$G_{23}$．这两个记号在下面说明，我们将证明二元戈莱码的扩展$G_{24}$是唯一的，由此可证$G_{23}$的唯一性．

**定理 20.5** *如果$C$是满足$|C|=2^{12}$、最小距离为8且长度为24的二元码，又$\boldsymbol{0}\in C$，则$C$等价于$G_{24}$．*

**证明** (i)困难的是证明$C$一定是一个线性码．为了明白这一点，观察删去任意一个坐标产生的长度为23、距离为7且$|C'|=2^{12}$的码$C'$．由问题20E，这个完全码的重量计数器被确定：$A_0=A_{23}=1$，$A_7=A_{16}=253$，$A_8=A_{15}=506$，$A_{11}=A_{12}=1288$．无论删去$C$的24个位置中的哪一个，都得到这一情形，由此得出$C$中所有码字的重量为0，8，12，16或24．此外，原始码字的改变(即所有的码字加上一个固定的码字)表明还可以推出任意两个码字的距离是0，8，12，16或24．因为所有的重量和所有的距离都$\equiv 0 \pmod 4$，任意两个码字的内积为

0. 所以 $C$ 的字张成一个自正交的码. 然而，这样的码至少有 $2^{12}$ 个字. 因此，$C$ 自身一定是一个线性的且自对偶的码.

254

(ii)通过取重量为 12 的任意一个字作为第一行构成 $C$ 的一个生成矩阵. 经过位置的一个排列之后，我们有

$$G=\begin{bmatrix}1 & \cdots & 1 & 0 & \cdots & 0\\ & A & & & B & \end{bmatrix}.$$

我们知道 $B$ 的行的任意线性组合一定有$\neq 0$ 的偶重量，于是 $B$ 的秩为 11. 因此由 $B$ 生成的码是[12, 11, 2]偶重量码. 我们得出这样的结论：可以假设 $B$ 是矩阵 $I_{11}$ 加宽了一列 1. 列的另一个排列产生形如$[I_{12}\quad P]$的生成矩阵 $G'$，这里 $P$ 与(20.13)中的形式相同. 关于矩阵 $N$ 我们知道什么？显然 $N$ 的任意一行的重量一定是 6. 此外，$N$ 的任意两行之和的重量至少是 6. 由问题 19D，$N$ 是唯一的 2-(11, 6, 3)设计的关联矩阵，即 $C$ 等价于 $G_{24}$. ■

正如我们在例 20.5 中看到的，在 $G_{24}$ 中重量为 8 的字构成维特设计 $\mathcal{D}=S(5, 8, 24)$的区组. 用$\{0, 1, \cdots, 23\}$表示 $\mathcal{D}$ 的点集并考虑 $I=\{21, 22, 23\}$. 由定理 19.3 的推论，$\mathcal{D}_I$ 是 $S(2, 5, 21)$，即阶为 4 的一个射影平面(已知它是唯一的). 下面的问题显示了设计 $\mathcal{D}$ 的优美的组合结构.

**问题 20H**　设 $B$ 是满足 $|B\cap I|=\alpha$ 的 $\mathcal{D}$ 的区组，定义 $B^*:=B\setminus I$. 可以看到如果 $\alpha=3$，则 $B^*$ 是 $PG_2(4)$中的一条线，证明：

(i)$\alpha=2$ 蕴涵 $B^*$ 在 $PG_2(4)$中是一个超卵形.

(ii)$\alpha=0$ 蕴涵 $B^*$ 是两条线的对称差.

(读者可能希望证明，如果 $\alpha=1$，则 $B^*$ 的七个点和包含 $B^*$ 的至少两个点的线构成一个费诺平面. 这样的平面称为 $PG_2(4)$的*白尔(Baer)子平面*.)

通过对超卵形、线对等进行计数，可以证明上面提到的每个几何构形是 $B^*$ 的一个集合. 事实上，$S(5, 8, 24)$的众所周知的构造之一就是以这些对象开始，通过附加 $I$ 的适当的子集产生这一设计. 如果在论证中不使用 $PG_2(4)$的自同构群，那么这个构造是一个非平凡的组合问题. (读者可以试一下.)

255

**问题 20I**　设$\mathbb{F}_4=\{0, 1, \omega, \bar{\omega}\}$. 设 $C$ 是$\mathbb{F}_4$ 上的[6, 3]码，具有码字$(a, b, c, f(1), f(\omega), f(\bar{\omega}))$，其中 $f(x):=ax^2+bx+c$.

(i)证明 $C$ 的最小重量是 4 且没有重量为 5 的字.

(ii)设 $G$ 是码字为所有 $4\times 6$ 的(0, 1)-矩阵 $A$ 的二元码，$A$ 的行 $\boldsymbol{a}_0$，$\boldsymbol{a}_1$，$\boldsymbol{a}_\omega$，$\boldsymbol{a}_{\bar{\omega}}$ 使得：

(1)$A$ 的每一列与其第一行 $\boldsymbol{a}_0$ 有相同的奇偶性.

(2)$\boldsymbol{a}_1+\omega\boldsymbol{a}_\omega+\bar{\omega}\boldsymbol{a}_{\bar{\omega}}\in C$.

证明 $G$ 是一个[24, 12, 8]码，即 $G=G_{24}$.

**问题 20J**　如在例 20.6 中，我们通过利用阶为 6 的 Paley 矩阵构造三元码 $Sym_{12}$. 证明 $Sym_{12}$ 是一个[12, 6, 6]自对偶码. 对这个码穿孔(即删去某个坐标)以得到一个[11, 6, 5]三元码 $G_{11}$. 证明这个码是完全的. 它是*三元戈莱码*.

现在，我们已经给出用适当的码构造设计的几个例子. 我们逆转这个过程并研究由一个设

计的区组(的特征函数)生成的码. 设 $N$ 是 $n$ 阶射影平面的关联矩阵. 考虑由 $N$ 的行生成的 $\mathbb{F}_2^v$ 的子空间 $C$，这里 $v=n^2+n+1$. 如果 $n$ 是奇数，则 $C$ 不令人感兴趣. 也就是说，如果我们取有一个固定位置为 1 的 $N$ 的行之和，结果是在这个位置上为 0 且在其他各处为 1 的一个行. 这些向量生成$[v, v-1, 2]$偶重量码，这个码一定是 $C$，因为显然 $C$ 没有奇重量的字. 如果 $n$ 为偶数，则问题变得更为有趣. 我们仅考虑 $n\equiv 2 \pmod 4$.

**定理 20.6** 如果 $n\equiv 2 \pmod 4$，$n$ 阶射影平面的关联矩阵的行生成维数为 $\frac{1}{2}(n^2+n+2)$ 的一个二元码 $C$.

**证明** (i)因为 $n$ 是偶数，由于每条线有奇数个点且任意两条线交于一点，所以码 $\bar{C}$ 是自正交的. 于是 $\dim C \leqslant \frac{1}{2}(n^2+n+2)$.

256

(ii)设 $\dim C=r$ 且 $k := n^2+n+1-r=\dim C^{\perp}$. 设 $H$ 为 $C$ 的奇偶校验矩阵. 假设坐标的位置以这样的方式排列，使得 $H$ 具有形式$(I_k\ P)$. 定义 $A := \begin{bmatrix} I_k & P \\ O & I_r \end{bmatrix}$. 把$(0, 1)$-矩阵 $N$ 和 $A$ 视为$\mathbb{Q}$上的矩阵. 则

$$\det NA^{\top} = \det N = (n+1)n^{\frac{1}{2}(n^2+n)}.$$

因为 $NA^{\top}$ 的前 $k$ 列的所有项是偶整数，显然 $\det N$ 能被 $2^k$ 整除. 于是 $\frac{1}{2}(n^2+n)\geqslant k$，即 $r\geqslant \frac{1}{2}(n^2+n+2)$.

由(i)和(ii)得到定理的结果. ■

这个定理表明由 $N$ 的行生成的码 $C$ 有 $\bar{C}$ 是自对偶的这一性质. 现在我们证明这个码的一个更有趣的性质，即可从这个码恢复射影平面.

**定理 20.7** 定理 20.6 中的码 $C$ 有最小重量 $n+1$ 且每个重量最小的码字对应 $n$ 阶平面上的一条线.

**证明** 如前所述，我们把一个码字看成平面的一个子集. 这样我们说一个点在一个码字 $\boldsymbol{c}$ 上的意义就很明确了. 设 $\boldsymbol{c}$ 是满足 $w(\boldsymbol{c})=d$ 的一个码字. 因为 $n$ 是偶数，所以与平面上的线对应的码字有一个 1 在扩展码 $\bar{C}$ 中作为奇偶校验符号. 码 $\bar{C}$ 是自对偶的且这蕴涵：

(1)如果 $d$ 是奇数，则 $\boldsymbol{c}$ 与每条线至少交于一次.

(2)如果 $d$ 是偶数，则穿过 $\boldsymbol{c}$ 的一个固定点的线与 $\boldsymbol{c}$ 交于第二个点.

在情形(2)我们马上看出 $d>n+1$. 在情形(1)我们发现：$(n+1)d\geqslant n^2+n+1$，即 $d\geqslant n+1$. 如果 $w(\boldsymbol{c})=n+1$，则平面上有一条线 $L$ 与 $\boldsymbol{c}$ 至少交于三个点. 如果 $L$ 上的某个点不是 $\boldsymbol{c}$ 中的点，由(1)穿过这个点且$\neq L$ 的每条线一定交于 $\boldsymbol{c}$. 这蕴涵着 $d\geqslant n+3$. 于是 $\boldsymbol{c}$ 必定是线 $L$. ■

回忆在偶数阶 $n$ 的一个射影平面上，*超卵形*是使得没有三点在一条线上的 $n+2$ 个点的集合.

257

**定理 20.8** 定理 20.6 的码 $C$ 中，重量为 $n+2$ 的码字正好是射影平面的所有超卵形.

**证明** (i)设 $\boldsymbol{v}\in C$ 且 $w(\boldsymbol{v})=n+2$. 每条线与 $\boldsymbol{v}$ 交于偶数个点. 设 $L$ 为射影平面上的一条

线，并假设$\boldsymbol{v}$和$L$有$2a$个公共点. $n$条$\neq L$的线中，每一条线穿过这$2a$个点之一至少与$\boldsymbol{v}$再相交一次. 因此$2a+n\leqslant n+2$，即$a=0$或$a=1$.

(ii)设$V$是一个超卵形. 又设$S$是$V$的$\binom{n+2}{2}$条割线的集合，不在$V$中的每个点在$\frac{1}{2}(n+2)$条这样的线上；$V$的每个点在$n+1$条割线上. 因为$n\equiv 2(\mathrm{mod}\ 4)$，对应于割线的码字的和是$V$的特征函数. 因此这是一个码字. ■

对与10阶的射影平面对应的码，与前两个定理类似的定理提供了足够的信息，使得前面提到的计算机搜索成为可能. 重要的第一步由 F. J. MacWilliams，N. J. A. Sloane，and J. G. Thompson(1973)迈出，他们证明这个码没有重量为15的字. 当前已知的阶为$n\equiv 2(\mathrm{mod}\ 4)$的射影平面只有费诺平面.

**问题 20K** 找出一个项为0，1和$-1$的$4\times 39$矩阵，使得(i)没有一列全是零且没有一列等于另一列乘以$\pm 1$，(ii)每一行包含13个0、13个1和13个$-1$.

推广到构造满足性质(i)和(ii)的$r\times\frac{1}{2}(3^r-1)-1$矩阵(13被适当的值所代替).

(上面的矩阵可用于如下的难题. 39个硬币中有一个假币，其重量大于或小于其余硬币. 给你一架有两个托盘的天平，一些硬币放入一个托盘，一些放入另一个托盘，天平会告诉你哪个子集有较大的总重量. 用四次称量，你必须确定出假币，以及它是较轻还是较重.)

**问题 20L** Körner 和 Simonyi 称$q>2$的字母表上的码为*三异码*，如果不仅码字不同，而且对码字的每个三元组，它们在某个位置有三个不同的项. 定义$F(n, q)$是一个长度为$n$的三异码的码字的最大数目. 证明$F(n, q)\geqslant 6^{-\frac{1}{2}}(q/3)^{n/2}$. (提示：利用定理3.6. 考虑一个有$N$个码字的随机码. 对$\{1, 2, \cdots, n\}$的每个3-子集$S$，设$A_S$是指标在$S$中的三个码字不全不相同或不是三异的事件. 证明$A_S$有概率$(3q(q-1)+q)^n/q^{3n}$，等等.)

258

## 评注

在本章中我们没有涉及码的纠错性质. 对编码理论的系统讨论，可参考 Van Lint(1999). 关于设计理论和编码理论之间关系的更多材料，可以参考 Cameron and Van Lint(1991). 编码理论的最佳参考书是 MacWilliams and Sloane(1977).

有关编码理论起源的历史，可以参考 Thompson(1983). 关于谁最先发明了这一理论存在争论，但是在1947年和1948年，汉明(R. W. Hamming)和戈莱(M. J. E. Golay)都对这一迷人课题的"发现"做出了贡献. C. E. Shannon(1948)的里程碑式的论文实际上启动了该课题. 似乎是汉明对他的计算机探测到一个错误时保持停顿而恼火. 他正确地推断，如果它能探测到错误，就应该能确定错误的位置并加以纠正，然后继续工作. 戈莱通过给出戈莱码的生成矩阵发表了两个戈莱码，但没有证明它们的性质.

E. F. Assmus(1931—1998)惨死在一次关于码和设计的会议上，会议在他喜爱的德国上沃尔法赫数学研究所举行. 本章的大部分内容基于他对编码理论和设计理论之间关系的许多贡献(文章多与 H. F. Mattson 合写).

戈莱(M. J. E. Golay，1902—1989)是瑞士物理学家，他在许多不同的领域工作．他以红外光谱学方面的工作和发明毛细柱而著名，但对数学他的发现主要是两种戈莱码．

关于 MDS 码的更多内容，参见 MacWilliams and Sloane(1977)．

F. J. MacWilliams(1917—1990)对编码理论做出了许多贡献．在这些贡献中，以她的名字而著称的定理是最重要的．她与 N. J. A. Sloane 合写的书是编码理论中最重要的参考书．与许多重要的编码理论家一样，她的大部分生涯在贝尔实验室度过． [259]

如前面提到的，有许多戈莱码 $G_{24}$ 的构造．每一种构造表明某个置换群包含在该码的自同构群中．例如，最常见的一个构造显示了一个 23 阶的自同构．因为这个码是唯一的，所以它的整个自同构群一定包含所有这些群作为子群．依这种方式，可以证明这个自同构群是著名的马蒂厄(Mathieu)群 $M_{24}$．这个群的阶为 $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$ 且 5-可迁地作用在码字的 24 个坐标位置上．

已经证明，除了本章提到的 $e>2$ 的完全 $e$-纠错码之外，不存在其他的完全 $e$-纠错码．关于这个主题的更多内容，见 Van Lint(1999)．也见第 30 章．

## 参考文献


E. F. Assmus, Jr. and H. F. Mattson, Jr. (1969), New 5-designs, *J. Combinatorial Theory* **6**, 122–151.

P. J. Cameron and J. H. van Lint (1991), *Designs, Graphs, Codes and their links*, London Math. Soc. Student Texts **22**, Cambridge University Press.

J. H. van Lint (1999), *Introduction to Coding Theory*, Third edition, Springer-Verlag.

F. J. MacWilliams (1963), A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.* **42**, 79–94.

F. J. MacWilliams and N. J. A. Sloane (1977), *The Theory of Error-Correcting Codes*, North-Holland.

F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson (1973), On the existence of a projective plane of order 10, *J. Combinatorial Theory* (A) **14**, 66–78.

V. Pless (1972), Symmetry codes over *GF*(3) and new 5-designs, *J. Combinatorial Theory* (A) **12**, 119–142.

C. E. Shannon (1948), A mathematical theory of communication, *Bell Syst. Tech. J.* **27**, 379–423 and 623–656.

T. M. Thompson (1983), *From Error-Correcting Codes through Sphere Packings to Simple Groups*, Carus Math. Monograph **21**.


[260]

# 第21章　强正则图和部分几何

强正则图 $srg(v,k,\lambda,\mu)$ 具有 $v$ 个顶点，次数 $k$ 是正则的，且满足下列性质：

(1)对任意两个相邻的顶点 $x$ 和 $y$，恰有 $\lambda$ 个顶点与 $x$ 和 $y$ 相邻.

(2)对任意两个不相邻的顶点 $x$ 和 $y$，恰有 $\mu$ 个顶点与 $x$ 和 $y$ 相邻.

一个平凡的例子是五边形——$srg(5,2,0,1)$. 也许最著名的例子是图 1.4 中的彼得森图——$srg(10,3,0,1)$.

显然 $m$ 个完全图 $K_k$ 的并是图 $srg(km,k-1,k-2,0)$. 有时我们通过要求一个强正则图和它的补是连通的来排除平凡的例子，即假设

$$0<\mu<k<v-1. \tag{21.1}$$

($\mu=0$ 蕴涵该图是完全图的并，这一事实极易从下面的(21.4)看出.)不难看出 $srg(v,k,\lambda,\mu)G$ 的补 $\overline{G}$ 是

$$srg(v,v-k-1,v-2k+\mu-2,v-2k+\lambda), \tag{21.2}$$

又因为参数是非负的，我们找到参数的一个简单条件，即

261

$$v-2k+\mu-2\geqslant 0. \tag{21.3}$$

不难发现，参数之间的另一个关系如下. 考虑任意一个顶点 $x$ 并将其他的顶点划分为：与 $x$ 相连的顶点的集合 $\Gamma(x)$，以及不与 $x$ 相连的顶点的集合 $\Delta(x)$. 由强正则图的定义，$\Gamma(x)$ 由 $k$ 个顶点组成，其中每一个顶点与 $\Gamma(x)$ 中的 $\lambda$ 个顶点相连. $\Delta(x)$ 中的每个顶点与 $\Gamma(x)$ 中的 $\mu$ 个顶点相连. 按两种方式对一端在 $\Gamma(x)$ 中另一端在 $\Delta(x)$ 中的边计数，我们发现

$$k(k-\lambda-1)=\mu(v-k-1). \tag{21.4}$$

**问题 21A**　证明：强正则图在如下的意义上是极图. 设 $G$ 有 $k$ 个顶点，每个顶点的次至多为 $k$. 假设任意两个相邻的顶点至少有 $\lambda$ 个公共的邻点，任意两个不相邻的顶点至少有 $\mu$ 个公共的邻点. 则

$$k(k-1-\lambda)\geqslant \mu(v-k-1),$$

等号成立蕴涵 $G$ 是强正则图.

在讲述这些图的迷人的理论之前，先给出几类例子.

**例 21.1**　三角形图 $T(m)(m\geqslant 4)$ 以基数为 $m$ 的集合的 2-元素子集作为顶点，两个不同的顶点相邻当且仅当它们不相交. $T(m)$ 是 $srg\left(\binom{m}{2},2(m-2),m-2,4\right)$. 彼得森图是 $\overline{T(5)}$ (见问题 1A).

**例 21.2**　格图 $L_2(m)(m\geqslant 2)$ 以 $S\times S$ 作为顶点的集合，这里 $S$ 是基数为 $m$ 的集合，两个不同的顶点相邻当且仅当它们有一个公共的坐标. $L_2(m)$ 是 $srg(m^2,2(m-1),m-2,2)$. $L_2(2)$ 是一个四边形，它是一个平凡的例子，因为 $\overline{L_2(2)}$ 不连通.

**例 21.3**　设 $q$ 是满足 $q\equiv 1(\mathrm{mod}4)$ 的素数幂. Paley 图 $P(q)$ 以 $\mathbb{F}_q$ 的元素作为顶点，两个顶点相邻当且仅当它们的差在 $\mathbb{F}_q$ 中是一个非零的平方. $P(q)$ 是 $srg(q,\frac{1}{2}(q-1),\frac{1}{4}(q-5),$

$\frac{1}{4}(q-1)$)，这是(18.4)的一个直接结果，但利用(18.5)的矩阵 $Q$ 易于证明这一点，正如下面我们将要看到的. 注意，$P(5)$是五边形. [262]

**例 21.4** 克莱布什(Clebsch)图的顶点是集合$\{1, \cdots, 5\}$的所有基数为偶数的子集，两个顶点相连当且仅当它们的对称差的基数为 4. 这是 $srg(16, 5, 0, 2)$. 也可以把顶点描述为$\mathbb{F}_2^5$中偶重量的字，如果两个字之间的距离为 4，这两个字对应的顶点有一条边相连. 对任意一个顶点 $x$，$\Delta(x)$的诱导子图是彼得森图. 见图 21.1.

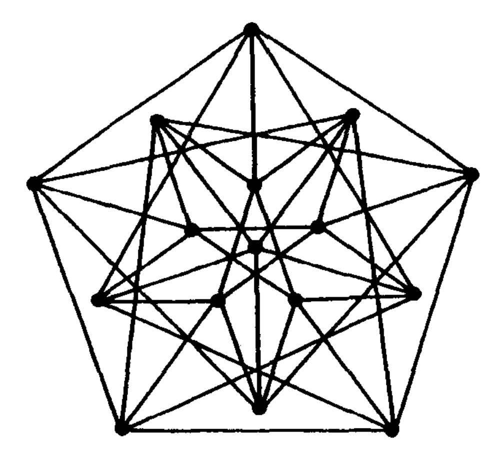


图 21.1

定义有 $v$ 个顶点 $1, \cdots, v$ 的图 $G$ 的邻接矩阵为 $v\times v$ 阶(0, 1)-矩阵，项 $a_{ij}=a_{ji}=1$ 当且仅当顶点 $i$ 和 $j$ 相连. 显然 $A$ 是对角线上为 0 的对称阵. $G$ 是 $srg(v, k, \lambda, \mu)$的表述等价于

$$AJ = kJ, \quad A^2+(\mu-\lambda)A+(\mu-k)I=\mu J. \tag{21.5}$$

如果 $Q$ 是(18.5)中出现的矩阵，则由(18.4)有 $Q^2=qI-J$，在例 21.3 中定义的图 $P(q)$的邻接矩阵是 $A=\frac{1}{2}(Q+J-I)$. 于是 $A$ 满足(21.5)且 $k=\frac{1}{2}(q-1)$，$\lambda=\frac{1}{4}(q-5)$，$\mu=\frac{1}{4}(q-1)$.

我们已经看到强正则图和前几章讨论过的主题之间的一个联系. 其他一些联系如下. 强正则图显示了与第 1～4 章和第 8 章讨论过的图论的一个完全不同的方面. 这里强烈地依赖代数方法. 然而，我们也希望显示计数方法在这一理论中的巧妙应用. [263]

定义一个 $srg\ G$ 的 Bose-Mesner 代数 $\mathfrak{A}$ 是 $I$，$J$ 和 $A$ 的线性组合的 3-维代数 $\mathfrak{A}$. 它确实是一个代数，这是(21.5)的一个结果. 这个代数由对称的交换矩阵构成，因此有一个正交矩阵同时对角化它们. 这也可以从(21.5)由初等方式看出. 事实上，在下一个定理中，我们将看到在$\mathbb{R}^v$中 $A$ 有三个不同的特征空间，而且其中每一个是 $\mathfrak{A}$ 的任何一个元素的特征空间.

**定理 21.1** *如果有一个图 $srg(v, k, \lambda, \mu)$，则数*

$$f := \frac{1}{2}\left\{v-1+\frac{(v-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2+4(k-\mu)}}\right\}$$

*和*

$$g := \frac{1}{2}\left\{v-1-\frac{(v-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2+4(k-\mu)}}\right\}$$

*是非负整数.*

**证明** 设 $A$ 为该图的邻接矩阵. 由(21.5)，全幺向量 $\boldsymbol{j}:=(1, 1, \cdots, 1)^{\top}$是 $A$ 的特征向量，具有特征值 $k$，当然它也是 $I$ 和 $J$ 的特征向量. (21.5)的应用产生(21.4)的第二个证明. 这个特征值的重数是 1，因为这个图是连通的. 任意其他特征向量，比如说特征值为 $x$ 的特征向量，与 $\boldsymbol{j}$ 正交，所以从(21.5)可以得到

$$x^2+(\mu-\lambda)x+(\mu-k)=0.$$

这个方程有两个解

264

$$r,s=\frac{1}{2}\{\lambda-\mu\pm\sqrt{(\lambda-\mu)^2+4(k-\mu)}\}. \tag{21.6}$$

设 $f$ 和 $g$ 是作为 $A$ 的特征值 $r$ 和 $s$ 的重数，则有

$$1+f+g=v \quad 且 \quad tr(A)=k+fr+gs=0. \qquad ■$$

如果解这两个线性方程，就得到定理的断言.

注意重数也可表示为

$$f=\frac{-k(s+1)(k-s)}{(k+rs)(r-s)} \quad 和 \quad g=\frac{k(r+1)(k-r)}{(k+rs)(r-s)}. \tag{21.7}$$

从(21.6)可以导出一个进一步的(令人惊奇的)结论. 如果 $f\neq g$，则在 $f$ 和 $g$ 的表达式中，分母中的平方根一定是整数，即$(\mu-\lambda)^2+4(k-\mu)$是一个完全平方. 从(21.6)得出特征值 $r$ 和 $s$ 都是整数！

另一种情形，即当 $f=g$ 时，通常称为半-情形. 那么我们有 $srg(4\mu+1, 2\mu, \mu-1, \mu)$. Paley 图是半-情形的例子. 在第 18 章提到的 Belevitch 关于会议电话的论文中，他观察到存在 $n$ 阶会议矩阵的一个必要条件是 $n-1$ 是两个平方数之和. 见问题 19M. 我们注意到参数 $v=21$，$k=10$，$\lambda=4$，$\mu=5$ 满足上述存在一个强正则图的所有必要条件，但不存在这样的图，因为利用(18.5)，它蕴涵存在一个 22 阶会议矩阵，由于 21 不是两个平方数之和，所以这是不可能的.

定理 21.1 的条件以整数性条件著称. 我们称满足这些条件及前面所述的必要条件的参数集$(v, k, \lambda, \mu)$为可行集.

**问题 21B** 证明：如果 $srg(k^2+1, k, 0, 1)$存在，则 $k=1, 2, 3, 7$ 或 57. (见第 4 章末的“评注”.)

我们已经看到 $srg(v, k, \lambda, \mu)$的邻接矩阵有三个特征值，其中之一是 $k$. 存在部分逆命题：如果 $G$ 是次为 $k$ 的连通正则图，它的邻接矩阵 $A$ 恰有三个不同的特征值，则 $G$ 是强正则的. 这是第 31 章的问题 31F.

265

为了获得强正则图的更多例子，我们考虑它与前面的一个主题——设计之间的联系. 这个想法属于 J. -M. Goethals and J. J. Seidel(1970). 一个 2-设计称为*拟对称的*，如果两个不同的区组的交的基数仅取两个不同的值，比如说 $x>y$. 我们引入一个图，称之为这个设计的区组图；图的顶点是该设计的区组，两个顶点相邻当且仅当它们的交的基数为 $y$.

**定理 21.2** *拟对称设计的区组图是强正则的.*

**证明** 设 $N$ 是该设计的 $v\times b$ 阶关联矩阵，且 $A$ 是其区组图 $G$ 的邻接矩阵. 我们有(利用 2-设计的参数 $v, k, b, r, \lambda$)：

$$NN^\top=(r-\lambda)I+\lambda J,$$
$$N^\top N=kI+yA+x(J-I-A).$$

(第一个方程是(19.7)，第二个方程是 $A$ 的定义.)我们知道 $NN^\top$ 和 $N^\top N$ 都有特征值 $kr$ 的全幺特征向量 $\mathbf{j}$(长度不同!). 我们还知道 $NN^\top$ 仅有重数为 $v-1$ 的 $\mathbf{j}^\perp$ 中的特征值 $r-\lambda$. 所以 $N^\top N$ 有相同的特征值且有相同的重数，以及重数为 $b-v$ 的特征值 0. 因为 $x\neq y$，$A$ 是 $I$，$J$

和 $N^{\top}N$ 的线性组合. 因此 $A$ 有特征向量 $j$ 且在空间 $j^{\perp}$ 中仅有两个特征值. 它们是重数为 $v-1$ 的 $(r-\lambda+k+x)/(y-x)$ 和重数为 $b-v$ 的 $(x-k)/(y-x)$. 由以上观察, 可知 $G$ 是强正则的. ■

既然我们已经知道 $G$ 是强正则的, 计算它的参数是很容易的. 这里不给出乏味的公式.

**例 21.5** 考虑第 20 章的 $S(5, 8, 24)$. 我们固定两个点并考虑相对于这两个点的剩余设计. 这是一个 3-(22, 6, 1). 从问题 20F 我们知道, 这个设计中包含一个给定点的 21 个区组是 $PG_2(4)$(即在该点移去之后)的线, 不包含这个点的 56 个区组是这个平面上的超卵形. 它们构成一个 2-(21, 6, 4)设计. 从 $S(5, 8, 24)$的性质得出两个超卵形交于 0 个或 2 个点. 因此, 这个导出设计是拟对称设计. 由定理 21.2, 该设计的区组图是$(56, k, \lambda, \mu)$. 这里 $k=10$, 因为有 $45=(4-1)\cdot\binom{6}{2}$个超卵形与一个给定的卵形交于 2 个点. 从该设计的性质或从强正则图的条件, 容易得出 $\lambda=0$, $\mu=2$. 这个例子中构造的图以 Gewirtz 图著称. 注意, 如果 $A$ 是 Gewirtz 图的邻接矩阵, 则由(21.5), 我们有$(I+A)^2=9I+2J$, 这意味着 $N:=I+A$ 是 2-(56, 11, 2)设计(一个所谓的双平面)的关联矩阵. 因此在这一情形, 我们也从强正则图找到一个新的设计.

[266]

**问题 21C** 设$\mathcal{D}:=(\mathcal{P}, \mathcal{B}, I)$是上面提到的 3-(22, 6, 1)设计; 它是唯一的. 我们构造一个顶点集为$\mathcal{P}\cup\mathcal{B}\cup\{\infty\}$的图. 顶点$\infty$与$\mathcal{P}$的每一个元素有边相连. $\mathcal{P}$的一个元素与$\mathcal{B}$的一个元素有边相连, 如果它们关联. 最后, $\mathcal{B}$的两个元素有边相连, 当且仅当这两个区组不相交. 证明这定义了 $srg(100, 22, 0, 6)$. 这个图称为 Higman-Sims 图.

如果此时列出强正则图的可行参数集表, 那么表中包含的许多集合没有对应的图. 下面证明排除这些集合的几个定理, 仍然使用代数方法. 作为准备, 读者应尽量尝试用纯组合论证明下面的问题.

**问题 21D** 证明不存在 $srg(28, 9, 0, 4)$.

这个图不存在是下面定理的一个结论, 这个定理以克赖因(Krein)条件著称.

**定理 21.3** 设 $G$ 是一个其邻接矩阵 $A$ 的特征值为 $k$, $r$ 和 $s$ 的强正则图, 则

$$(r+1)(k+r+2rs)\leqslant(k+r)(s+1)^2$$

和

$$(s+1)(k+s+2sr)\leqslant(k+s)(r+1)^2.$$

[267]

**证明** 设 $B:=J-I-A$. 我们知道 $\mathfrak{A}$ 的矩阵有维数分别为 1, $f$ 和 $g$ 的三个公共的特征空间. 称这些空间为 $V_0$, $V_1$ 和 $V_2$. 这里 $V_0$ 是由 $j$ 张成的空间, $V_1$ 和 $V_2$ 对应于 $A$ 的特征值 $r$ 和 $s$. 对 $i=0, 1, 2$, 设 $E_i$ 是 $V_i$ 上的射影矩阵, 即 $E_i$ 在 $V_i$ 上的特征值为 1 且在其他两个特征空间中为 0. 这些矩阵称为 $\mathfrak{A}$ 的一组最小幂等基. 现在考虑同一个集合 $\mathfrak{A}$, 但作为乘法我们考虑阿达马积(见问题 21E). 显然, $I$, $A$ 和 $B$ 中的任意两个的积为 $O$. 任意(0, 1)-矩阵对阿达马乘法是幂等的. 于是我们得出 $\mathfrak{A}$ 在阿达马乘法下是封闭的, 矩阵 $I$, $A$ 和 $B$ 是一组最小幂等基.

注意 $E_i(i=0, 1, 2)$的定义蕴涵

$$I=E_0+E_1+E_2,\quad A=kE_0+rE_1+sE_2$$

和

$$B=(v-k-1)E_0+(-r-1)E_1+(-s-1)E_2.$$

由此，可以用 $I$，$A$ 和 $B$ 表示 $E_i$.

考虑矩阵 $E_i$ 在阿达马积下的表现．因为它们构成 $\mathfrak{A}$ 的一组基，我们有

$$E_i\circ E_j=\sum_{k=0}^{2}q_{ij}^{k}E_k,$$

这里 $q_{ij}^k$ 是 $E_i\circ E_j$ 在 $V_k$ 上的特征值．经过冗长的计算，利用上面给出的关系，数 $g_{ij}^k$ 可以用 $G$ 的参数表示.

此时我们需要问题 21E 的结果．阿达马积 $E_i\circ E_j$ 是克罗内克积 $E_i\otimes E_j$ 的主子矩阵．这个矩阵是幂等的，因此其特征值是 0 和 1．在问题 21E 中这个定理已暗示了，特征值 $q_{ij}^k$ 一定在 0 和 1 之间．(在做完所有的计算之后)得出：按这种方式找到的不等式中除两个之外都是满足条件的，那两个不等式是 $q_{11}^1\geqslant 0$ 和 $q_{22}^2\geqslant 0$．它们就是断言中的两个方程. ■

268

**问题 21E** 设 $A$ 和 $B$ 是特征值分别为 $\lambda_1$，…，$\lambda_n$ 和 $\mu_1$，…，$\mu_n$ 的两个 $n\times n$ 对称矩阵．确定 $A\otimes B$ 的特征值．我们定义 $A$ 和 $B$ 的阿达马积 $A\circ B$ 是项为 $a_{ij}b_{ij}$ 的矩阵．证明 $A\circ B$ 是 $A\otimes B$ 的主子矩阵．关于 $A\circ B$ 的特征值你能得出什么结论？

为了体会下一个定理，读者应首先确信参数集(50，21，4，12)是可行的，而且它满足克赖因条件．为了证明这个集合不对应一个强正则图应对什么进行计数？

**定理 21.4** *设 $srg(v, k, \lambda, \mu)$ 的邻接矩阵 $A$ 的特征值为 $k$，$r$，$s$，并且设它们的重数是 1，$f$ 和 $g$，则*

$$v\leqslant\frac{1}{2}f(f+3)\quad 和\quad v\leqslant\frac{1}{2}g(g+3).$$

**证明** 设 $B$ 等于 $J-I-A$ 且矩阵 $E_i(i=0, 1, 2)$ 与前一个定理证明中的相同．设

$$E_1=\alpha I+\beta A+\gamma B.$$

因为 $E_1$ 是对称的，存在一个正交矩阵 $[H_1\quad K_1]$ 使得

$$E_1=[H_1\quad K_1]\begin{bmatrix}I & O\\ O & O\end{bmatrix}\begin{bmatrix}H_1^{\top}\\ K_1^{\top}\end{bmatrix}=H_1H_1^{\top}.$$

这里 $H_1$ 是满足 $H_1^{\top}H_1=I$ 的 $v\times f$ 矩阵．我们把 $H_1$ 的行看成 $\mathbb{R}^f$ 中的 $v$ 个向量．由此这些向量中的每一个有长度 $\alpha^{\frac{1}{2}}$，这个集合(称之为 $S$)中两个不同向量的内积为 $\beta$ 或 $\gamma$．这样的集合称为*球的 2-距离集*，因为可以把 $S$ 理解为在一个球中只有两个不同的(角)距离的点集．我们必须证明 $S$ 的基数至多为 $\frac{1}{2}f(f+3)$.

加以规范化，得到在 $\mathbb{R}^f$ 中单位球 $\Omega$ 上的 $v$ 个向量的一个集合 $S'$，向量仅有两个内积，比如说设为 $b$ 和 $c$．对每个 $\boldsymbol{v}\in S'$，由

$$f_{\boldsymbol{v}}(\boldsymbol{x}):=\frac{(\langle\boldsymbol{v},\boldsymbol{x}\rangle-b)(\langle\boldsymbol{v},\boldsymbol{x}\rangle-c)}{(1-b)(1-c)}$$

269

定义一个函数 $f_{\boldsymbol{v}}:\Omega\to\mathbb{R}$．这些函数是 $\boldsymbol{x}$ 坐标的 2 次多项式．如果 $\boldsymbol{v}\in S$，$\boldsymbol{w}\in S$ 且 $\boldsymbol{v}\neq\boldsymbol{w}$，则 $f_{\boldsymbol{v}}(\boldsymbol{v})=1$ 且 $f_{\boldsymbol{v}}(\boldsymbol{w})=0$．因此，这些函数是线性无关的．$\Omega$ 上齐次线性型和齐次二次型的空

间分别有维数 $f$ 和 $\frac{1}{2}f(f+1)$；因为在 $\Omega$ 上 $x_1^2+\cdots+x_f^2=1$，所以可以用 2 次型和 1 次型表示常数．由函数 $f_v$ 的线性无关性可知，它们至多有 $f+\frac{1}{2}f(f+1)=\frac{1}{2}f(f+3)$ 个． ■

这个定理以绝对界著称．A. Neumaier(1980)证明这个绝对界可改进为

$$v\leqslant\frac{1}{2}f(f+1),\quad 除非\ q_{11}^1=0$$

(对另一个不等式有类似的改进)．

在讨论强正则图和特定的关联结构之间的关系之前，我们证明好的计数论证在这一领域也很有用．

**定理 21.5** 设 $G$ 是一个与 $T(n)$ 有相同参数的强正则图，即 $G=srg\left(\binom{n}{2},\ 2(n-2),\ n-2,\ 4\right)$．如果 $n>8$，则 $G$ 同构于 $T(n)$．

**证明** 固定一个顶点 $x$，用 $\Gamma$ 表示 $\Gamma(x)$ 上的诱导子图．这是一个有 $2(n-2)$ 个顶点、次为 $n-2$ 的正则图．设 $y$ 和 $z$ 是 $\Gamma$ 的不相邻顶点，并且设在 $\Gamma$ 中有 $m$ 个顶点与这两个点相邻．因为 $\mu=4$ 且 $x$ 与 $y$ 和 $z$ 相邻，我们有 $m\leqslant 3$．在图 $\Gamma$ 中，有 $n-2-m$ 个顶点与 $y$ 相邻但不与 $z$ 相邻，且有同样多的顶点仅与 $z$ 相邻．因此有 $m-2$ 个顶点既不与 $y$ 相邻也不与 $z$ 相邻．于是 $m\geqslant 2$. 假设 $m=3$，考虑唯一的既不与 $y$ 又不与 $x$ 相邻的顶点 $w$．在 $\Gamma$ 中与 $w$ 相邻的顶点与 $y$ 或者 $z$ 相邻，这蕴涵着 $n-2\leqslant 3+3=6$，矛盾．因此 $m=2$，并且我们还看到在补 $\bar{\Gamma}$ 中没有三角形．

现在我们证明 $\bar{\Gamma}$ 是二部图．反之，假设在这个图中有奇数长度的一个回路．选择这样的回路 $C=(x_0,\ x_1,\ \cdots,\ x_k=x_0)$ 使 $k$ 最小．从上面的论证我们知道 $k\neq 3$．在图 $\Gamma$ 中，顶点 $x_0$ 和 $x_1$ 不相邻且都与 $x_3,\ x_4,\ \cdots,\ x_{k-2}$ 相邻．由上面的论证可知 $k\leqslant 6$，又因为 $k$ 是奇数，$k=5$．$x_0$ 在 $\bar{\Gamma}$ 中的次数为 $n-3$，即它与除 $x_1$ 和 $x_4$ 之外的 $n-5$ 个点相邻．在 $\bar{\Gamma}$ 中一定有既不与 $x_1$ 又不与 $x_4$ 相邻的点．对 $x_2$ 可作类似的断言，产生 $C$ 之外的 $n-5$ 个点在 $\bar{\Gamma}$ 中既不与 $x_1$ 也不与 $x_3$ 相邻．$C$ 之外恰有 $n-4$ 个顶点不与 $x_1$ 相邻；因此在 $\bar{\Gamma}$ 中至少有 $n-6$ 个顶点既不与 $x_3$ 也不与 $x_4$ 相邻．第一段的结果蕴涵 $n-6\leqslant 1$，矛盾． [270]

第二段的结果意味着 $\Gamma$ 包含两个不相交的团(点的集合，团中的任意两个点相邻)，团的规模为 $n-2$．因为 $x$ 是任意的，我们已经证明 $G$ 中的任意一个顶点位于规模为 $n-1$ 的两个团中(这样规模的团称为大团)．同样的论证证明任意一条边在这些大团之一中．大团的数目是 $2\binom{n}{2}/(n-1)=n$．因为任意两个大团至多有一个公共顶点，所以它们一定恰有一个公共顶点．如果把大团作为"点"且把顶点作为"区组"，那么我们刚才证明了这些点和区组构成一个 $2$-$(n,\ 2,\ 1)$设计，即所有的对子形成一个 $n$-集合的平凡设计．$G$ 是这个设计的区组图，即 $G$ 的确同构于 $T(n)$． ■

我们说由情形分析，对 $n<8$ 和 $n=8$ 亦可证明该定理，当 $n=8$ 时，有满足 $T(8)$ 的参数的另外三个图，称为张图．

**问题 21F** 设 $G$ 是一个与 $L_2(n)$ 具有相同参数的强正则图，即 $G=srg(n^2, 2(n-1), n-2, 2)$. 证明：如果 $n>4$，则 $G$ 同构于 $L_2(n)$.

R. C. Bose(1963)在更一般的强正则图中研究了大团. 这把他引向部分几何的概念. 部分几何 $pg(K, R, T)$ 是一个具有如下性质的点和线的关联结构：

(1)每条线有 $K$ 个点且每个点在 $R$ 条线上.

(2)任意两个点至多与一条线关联.

271 (3)如果点 $p$ 不在线 $L$ 上，则恰有 $T$ 条线穿过 $p$ 与 $L$ 相交.

如果两个点 $x$ 和 $y$ 在一条线上，我们说它们是共线的，并写作 $x\sim y$.

**问题 21G** 确定一个部分几何 $pg(K, R, T)$ 中点和线的数目.

在一个部分几何 $pg(K, R, T)$ 中，交换点和线的角色，可以得到所谓的对偶部分几何——$pg(R, K, T)$.

我们引入一个部分几何的点图：该几何的点作为顶点，边为 $\{x, y\}$ 当且仅当 $x\sim y$.

**问题 21H** 证明一个 $pg(K, R, T)$ 的点图是满足

$$v=K\left(1+\frac{(K-1)(R-1)}{T}\right),\quad k=R(K-1),$$
$$\lambda=(K-2)+(R-1)(T-1),\quad \mu=RT,$$
$$r=K-1-T,\quad s=-R$$

的(可能是平凡的)$srg(v, k, \lambda, \mu)$.

如果一个强正则图的参数使得该图可能是某一部分几何的点图，那么称这个图是伪几何的，如果它确实是一个部分几何的点图，则称这个图是几何的. 引入大团，并证明大团和点构成一个设计，这一想法被 Bose 用来证明下面的定理.

**定理 21.6** 如果一个强正则图是伪几何的，它对应 $pg(K, R, T)$，如果 $2K>R(R-1)+T(R+1)(R^2-2R+2)$，则该图是几何的.

这里我们不给出该定理的证明. 这个证明的想法被 A. Neumaier(1979)所扩展，在经 272 A. E. Brouwer 改进之后，他的结果获得了如下形式(以爪界著称).

**定理 21.7** 对一个有通常参数的强正则图，如果 $\mu\neq s^2$ 且 $\mu\neq s(s+1)$，则 $2(r+1)\leqslant s(s+1)(\mu+1)$.

这个定理的证明思路是，如果 $r$ 较大，则可由计数论证得到这个图是一个部分几何的点图，然后把绝对界以及克赖因条件用于对偶部分几何的点图. 这表明所叙述的不等式中，$r$ 不能太大.

参数(2058, 242, 91, 20)是可行的且满足除爪界之外本章所述的所有必要条件. 因此，不存在具有这些参数的图.

**问题 21I** 考虑 $srg(v, k, \lambda, 1)$. 证明 $\Gamma(x)$ 上的诱导子图是团的并. 计算图中$(\lambda+2)$-团的数目. 由此证明 $k/(\lambda+1)$ 和 $vk/\{(\lambda+1)(\lambda+2)\}$ 都是整数. 将它用于集合(209, 16, 3, 1).

部分几何可以分为以下四类：

(1)满足 $T=K$ 的部分几何是一个 2-$(v, K, 1)$设计.

(2)满足 $T=R-1$ 的部分几何称为网；对偶地，如果 $T=K-1$，称之为横截设计.

(3) 满足 $T=1$ 的部分几何称为广义四边形；记号 $GQ(K-1, R-1)$ 通常用于 $pg(K, R, 1)$.

(4) 如果 $1<T<\min\{K-1, R-1\}$，则称部分几何是正常的.

**例 21.6** 考虑仿射平面 $AG_2(n)$. 从问题 19K 我们知道它的线可以分成平行线的等价类，每一个类包含 $n$ 条线. 考虑平面上所有的点并取 $m$ 个平行类的线. 显然，这些点和线构成一个 $pg(n, m, m-1)$，即一张网.

**例 21.7** 考虑 $n$ 阶拉丁方. 设 $n^2$ 个腔是图的顶点；两个顶点由一条边相连当且仅当它们在同一行或同一列，或者它们有相同的项. 该图是次为 $3(n-1)$ 的正则图. 如果两个顶点被连结，不失一般性，可以假设它们在同一行(把这个拉丁方看成 $OA(n, 3)$). 那么它们有 $n-2$ 个相互的邻点. 如果两个顶点不相连，则显然它们有六个公共的邻点. 因此这是一个 $srg(n^2, 3(n-1), n-2, 6)$. 这个图称为拉丁方图，记作 $L_3(n)$，与例 21.2 的记号相符. 在后面将有推广. 图 $L_3(n)$ 是几何的，对应部分几何 $pg(n, 3, 2)$，即一张网. 当然，线对应拉丁方的行、列和符号. 在第 22 章中我们将看到网和正交阵列等价的概念. [273]

**例 21.8** 一个四边形满足部分几何的条件. 这是 $pg(2, 2, 1)$，它解释了名字“广义四边形”.

考虑 $PG_2(4)$ 上的一个超卵形 $O$. 我们取不在 $O$ 上的平面的 15 个点为点集. 线是 $O$ 的割线. 那么每条线有 3 个点，且每个点在 3 条线上，事实上这是 $pg(3, 3, 1)$，即 $GQ(2, 2)$.

注意，相同的构造应用于 $q$ 为偶数的 $PG_2(q)$ 产生 $pg\left(q-1, \frac{1}{2}(q+2), \frac{1}{2}(q-2)\right)$.

**例 21.9** 考虑 $q$ 为偶数的 $PG_2(q)$. 如在例 19.7 中，这是一个关联结构，其对象为 $\mathbb{F}_q^3$ 的 1-维子空间和 2-维子空间. 又设 $O$ 为射影平面上的一个超卵形. 设 $O$ 中的所有 1-维子空间和它们在 $\mathbb{F}_q^3$ 中的陪集是线；点是向量空间中的点. 每条线有 $q$ 个点，每个点在 $q+2$ 条线上. $O$ 是一个超卵形蕴涵着对任意不在线 $L$ 上的点 $p$，有唯一的一条线穿过 $p$ 与 $L$ 相交. 于是我们已经定义了 $GQ(q-1, q+1)$.

**例 21.10** 考虑由元素 $(1, 1, 1, 1, 1, 1)$ 生成的 $\mathbb{Z}_3^6$ 的子群 $G$. 对每个陪集 $\boldsymbol{a}+G$，其中点的坐标之和是常数 $i$. 我们说该陪集属于类型 $i$. 设 $\mathcal{A}_i$ 为 $G$ 的类型为 $i$ 的陪集的集合. 对每个只有一个非零坐标的 $\boldsymbol{b}$，通过连结陪集 $\boldsymbol{a}+G$ 和陪集 $\boldsymbol{a}+\boldsymbol{b}+G$ 定义一个三部图 $\Gamma$. 显然，$\mathcal{A}_i$ 的每个元素在 $\mathcal{A}_{i+1}$ 中有 6 个相邻元素且在 $\mathcal{A}_{i+2}$ 中有 6 个相邻元素. 取某个 $\mathcal{A}_i$ 作为点集，两个类 $\mathcal{A}_j$ 中的一个作为线集，构造一个部分几何. 关联对应相邻. 显然，$K=R=6$. 很容易证明 $T=2$. 这定义了一个 $pg(6, 6, 2)$. [274]

下面给出定理 21.5 的一个不错的应用. 我们将证明在第 19 章提到但没给出证明的一个定理，它断言 $\lambda=2$ 的拟剩余设计是剩余设计. 因为 $k\leqslant 6$ 的情形需要分开讨论，所以我们限制区组的规模 $>6$.

**定理 21.8** *设 $\mathcal{D}$ 是一个满足 $k>6$ 且 $v=\frac{1}{2}k(k+1)$ 的 2-$(v, k, 2)$ 设计(于是 $\mathcal{D}$ 是拟剩余的)，则 $\mathcal{D}$ 是一个对称 2-设计的剩余.*

**证明** 设 $B$ 为一个区组，且设 $a_i$ 表示与 $B$ 交于 $i$ 个点的($\neq B$ 的)区组数. 如在定理 19.9

中，我们发现

$$\sum a_i=\frac{1}{2}k(k+3),\quad \sum ia_i=k(k+1),\quad \sum i(i-1)a_i=k(k-1).$$

这蕴涵$\sum(i-1)(i-2)a_i=0$. 因此，任意两个不同的区组交于 1 个或 2 个点，即设计$\mathcal{D}$是拟对称的. 从定理 21.2 我们发现$\mathcal{D}$的区组图 $G$ 是强正则的. 对参数的计算表明 $G$ 与 $T(k+2)$的参数相同. 因此，由定理 21.5，$G$ 与 $T(k+2)$同构. 这意味着可以按这种方式用 $S:=\{1, 2, \cdots, k+2\}$的 2-子集标记$\mathcal{D}$的区组，使得当两个区组的标记交于$2-i(i=1, 2)$个点时，它们交于 $i$ 个点. 把集 $S$ 毗连到$\mathcal{D}$的点集上，每个区组毗连其标号，即 $S$ 的一个 2-子集. 最后，把 $S$ 作为一个新的区组考虑. 这产生满足 $\lambda=2$ 所要求的对称设计，它有$\mathcal{D}$作为相对于区组 $S$ 的剩余. ■

下表列出 $v<30$ 的可行参数集及本章所讲述的有关它们的内容. 唯一留给读者的是 14 号，即 $GQ(2, 4)$，它的构造没有给出. 它对应的图称为 Schlaefli 图.

275

| 编号 | $v$ | $k$ | $\lambda$ | $\mu$ | 例子 |
|---|---|---|---|---|---|
| 1 | 5 | 2 | 0 | 1 | $P(5)$ |
| 2 | 9 | 4 | 1 | 2 | $L_2(3)$ |
| 3 | 10 | 3 | 0 | 1 | 彼得森，$\overline{T(5)}$ |
| 4 | 13 | 6 | 2 | 3 | $P(13)$ |
| 5 | 15 | 6 | 1 | 3 | $GQ(2, 2)$ |
| 6 | 16 | 5 | 0 | 2 | 克莱布什 |
| 7 | 16 | 6 | 2 | 2 | $L_2(4)$ |
| 8 | 17 | 8 | 3 | 4 | $P(17)$ |
| 9 | 21 | 10 | 3 | 6 | $T(7)$ |
| 10 | 21 | 10 | 4 | 5 | 不存在，会议 |
| 11 | 25 | 8 | 3 | 2 | $L_2(5)$ |
| 12 | 25 | 12 | 5 | 6 | $L_3(5)$ |
| 13 | 26 | 10 | 3 | 4 | $STS(13)$，定理 21.2 |
| 14 | 27 | 10 | 1 | 5 | $GQ(2, 4)$ |
| 15 | 28 | 9 | 0 | 4 | 不存在，定理 21.3 和定理 21.4 |
| 16 | 28 | 12 | 6 | 4 | $T(8)$ |
| 17 | 29 | 14 | 6 | 7 | $P(29)$ |

下面给出有向强正则图的几个注释和一些例子.

在强正则图的定义中，关于长度为 2 的路的条件，把(21.5)写成

$$AJ=kJ,\quad A^2=kI+\lambda A+\mu(J-I-A) \tag{21.5'}$$

来看最好. 这个定义被 A. Duval(1988)推广到有向图. 考虑一个没有环或重边的有向图 $G$. 如果从 $a$ 到 $b$ 有一条边，则写成 $a\to b$. 我们允许两个方向的边，用 $a\leftrightarrow b$ 表示. 在这种情形称$(a, b)$为无向边. 相对于长度为 2 的路，(21.5′)的推广不变，但是需要每个点有入次 $k$、出次 $k$，且在这些边中有 $t$ 条无向边(从一个点自身产生长度为 2 的路). 这样，$G$ 称为有向强正则

图，如果其邻接矩阵 $A$ 满足

$$AJ = JA = kJ, \quad A^2 = tI + \lambda A + \mu(J - I - A). \tag{21.8}$$

276

对于有 $v$ 个顶点的这样的图，用记号 $dsrg(v; k, t; \lambda, \mu)$来表示.

**例 21.11** 设 $G$ 为有 6 个顶点的图，它由有向三角形 $1 \to 2 \to 3 \to 1$ 和 $1' \to 3' \to 2' \to 1'$，及无向边$(i, i')$构成，$i=1, 2, 3$. 如果 $C$ 是 $3\times 3$ 循环矩阵，对$(i, j)=(1, 2), (2, 3), (3, 1)$，项 $c_{ij}$ 等于 1，其他情况项 $c_{ij}$ 为 0，则 $G$ 的邻接矩阵 $A$ 为

$$A = \begin{bmatrix} C & I \\ I & C^2 \end{bmatrix}.$$

容易验证，当 $k=2$，$t=1$，$\lambda=0$ 和 $\mu=1$ 时，$A$ 满足(21.8). 于是 $G$ 是 $dsrg(6; 2, 1; 0, 1)$.

**问题 21J** 对有向强正则图，叙述并证明与定理 21.1 类似的情况.

**问题 21K** 排除有邻接矩阵 $J-A$ 的强正则图和图. 证明在问题 21J 中计算的特征值导致"半-情形"的类似物，如果$(\mu-\lambda)^2+4(t-\mu)$不是一个整数的平方. 证明在这种情形. 这个 $dsrg$ 的邻接矩阵 $A$ 是(18.5)中 $Q$ 的类型.

**问题 21L** 考虑 $\mu=1$，$\lambda=0$，$t=k-1$ 的情形. 证明 $v$ 只有三个可能的值. 证明在第二种情形，通过把 $K_{3,3}$的顶点用有向三角形代替，以适当的方式拷贝例 21.11 的图代替边，能得到一个例子.

下面给出关于邻域正则图的几则评论和问题.

强正则图 $G$ 中 $x$ 的邻域 $\Gamma(x)$和补图 $\bar{G}$ 中 $x$ 的邻域 $\Delta(x)$都是正则图. C. D. Godsil and B. D. McKay(1979)称有这一性质的图为邻域正则图. 不难证明邻域正则图也是正则的，事实上它是强正则图. 如果 $G$ 或 $\bar{G}$ 不连通时出现平凡的情形. 在下面的问题中，我们假设 $G$ 是邻域正则的，但不是正则的，且 $G$ 和 $\bar{G}$ 都是连通的.

277

**问题 21M** (i)证明 $\Gamma(x)$的次不依赖 $x$. 称这个数为 $a$.

(ii)证明存在一个数$\bar{a}$使得对每个 $x$，$\overline{\Delta(x)}$的次是$\bar{a}$.

**问题 21N** 如果 $X$ 和 $Y$ 是$G$ 的顶点集的子集，我们用 $|XY|$ 表示 $G$ 中 $x\in X$ 且 $y\in Y$ 的边$(x, y)$的数目. 设 $x_1$ 和 $x_2$ 是 $G$ 中次数分别为 $k_1$ 和 $k_2$ 的两条不相邻的边，$k_1\neq k_2$. 又设 $d_i := \deg\Delta(x_i)$，$i=1, 2$. 注意，$d_1\neq d_2$. 现在考虑如下 $G$ 的顶点集的子集：$A := \Gamma(x_1)\cap\Delta(x_2)$，$B := \Gamma(x_2)\cap\Delta(x_1)$，$C := \Gamma(x_1)\cap\Gamma(x_2)$，$D := \Delta(x_1)\cap\Delta(x_2)$.

(i)寻找数 $|XY|$ 和 $|X|$ 之间的关系，这里 $X$ 和 $Y$ 取自 $B$，$C$，$D$.

(ii)导出

$$|DD| = (a+\bar{a}+1)d_1 - d_1^2 - a|C| + |CC|.$$

(iii)证明 $d_1+d_2=a+\bar{a}+1$.

(iv)证明 $G$ 中所有顶点的次为 $k_1$ 或 $k_2$.

**例 21.12** 设 $G$ 是点 1 到 8 上的八边形且有两条对角线(15)和(26). 这是 $k_1=2$，$k_2=3$，$a=0$，$\bar{a}=2$，$d_1=1$ 且 $d_2=2$ 的邻域正则图.

**问题 21O** 给定一个 $n$ 个点上的施泰纳三元系$S$，定义一个图 $G$，它的顶点是该系的三元

组$\mathcal{A}$，这里当$|A\cap B|=1$时，$A$，$B\in\mathcal{A}$是相邻的.

(i)用初等方法(即不用定理 21.2 或矩阵方法)证明$G$是强正则的，并计算其参数.

(ii)证明：如果在$G$中$C$是一个$|C|>7$的团，则$C$是三元组的一个子集，对$\mathcal{S}$的某个点$x$，它包含一个固定的点$x$.

(iii)利用这个结论证明：如果来自$n>15$个点上的两个施泰纳系的图$G_1$和$G_2$是同构的，则这两个系也是同构的.（注意，在 25 个点上有超过 163 929 929 318 400 个不同构的施泰纳三元系——见 R. M. Wilson(1973/74)——因此，在 100 个顶点上至少有这么多不同构的强正则图.）

278

**问题 21P** 证明问题 4H 中的等号不成立，除非$n=3$.

**问题 21Q** 证明所谓的*友谊定理*：在一个$n$个人($n>3$)的聚会上，每两个人恰有一个共同的朋友. 那么在这个聚会上有唯一的一个人，他是所有其他人的朋友. 利用问题 1J.

## 评注

强正则图和部分几何在 1963 年由 R. C. Bose 引入. 一个更一般的概念，即*结合方案*，由 Bose 和 Shimamoto 在 1952 年引入；见本书的第 30 章和 Cameron and Van Lint(1991)，第 17 章.

强正则图构造方法的一个概述，见 Hubaut(1975)和 Brouwer and Van Lint(1982).

克莱布什图可以由克莱布什四次曲线上的 16 条线定义，一对线是相邻的当且仅当它们是偏斜的. 克莱布什(Alfred Clebsch，1833—1872)是数学家和物理学家，他在德国卡尔斯鲁厄、吉森和哥廷根工作. 他是著名杂志《Mathematische Annalen》的创刊人之一.

代数$\mathfrak{A}$由 R. C. Bose 和 D. M. Mesner 在 1959 年引入.

除了定理 21.2，Goethals and Seidel(1970)包含强正则图和其他组合设计之间的许多有趣联系. 阿达马矩阵、施泰纳系和戈莱码都对这一理论有贡献. 对这些联系，又见 Cameron and Van Lint(1991).

Higman-Sims 图与著名的有限简单群相联系(见 Higman and Sims(1968)).

定理 21.3 的一个特殊情形被 L. L. Scott 用克赖因(M. G. Krein)关于有限群的一个问题的拓扑群的结果证明，因此该定理以克赖因条件著称. 本章给出的简单证明属于 D. G. Higman (1975)和 P. Delsarte(1973). 在克赖因条件中等式成立的情况参见 Delstarte，Goethals and Seidel(1977)，以及 Cameron，Goethals and Seidel(1978).

279

定理 21.4 的证明思路属于 T. H. Koornwinder(1976).

定理 21.5 数次被证明：例如，参见 L. C. Chang (1959)、W. S. Connor (1958) 和 A. J. Hoffman(1960). $n=8$时的三个例外图以张图著称.

部分几何的综述见 Van Lint(1983)、De Clerck and Van Maldeghem(1995)，以及 De Clerck(2000).

网由 R. H. Bruck 在 1951 年引入. Bose 关于伪几何图的结果是从 Bruck 的工作得到的灵感(例如，大团的概念).

想了解广义四边形(及其他)的读者，可参考 S. E. Payne 和 J. A. Thas 于 1984 年所著的书

《Finite Generalized Quadrangles》.

$T=2$ 时只知道三个正常的部分几何. 例 21.9 中的几何 $pg(6, 6, 2)$ 首先由 Van Lint and Schrijver(1981)构造；我们描述的构造属于 Cameron and Van Lint(1982). 其他已知的例子中，$pg(5, 18, 2)$ 属于 Haemers，$pg(8, 20, 2)$ 由 Mathon(借助计算机)发现.

第 19 章提到的 10 阶射影平面的不存在性，通向其证明的一大步是不存在 $pg(6, 9, 4)$ 的证明. 这蕴涵(见例 21.8)着，如果这个平面存在，它将没有超卵形.

## 参考文献


R. C. Bose (1963), Strongly regular graphs, partial geometries, and partially balanced designs, *Pacific J. Math.* **13**, 389–419.

R. C. Bose and D. M. Mesner (1959), On linear associative algebras corresponding to association schemes of partially balanced designs, *Ann. Math. Stat.* **30**, 21–38.

A. E. Brouwer and J. H. van Lint (1982), Strongly regular graphs and partial geometries, in: *Enumeration and Design* (D. M. Jackson and S. A. Vanstone, eds.), Academic Press.

R. H. Bruck (1951), Finite nets I, *Canad. J. Math.* **3**, 94–107.

R. H. Bruck (1963), Finite nets II, *Pacific J. Math.* **13**, 421–457.


280


P. J. Cameron (1978), Strongly regular graphs, in: *Selected Topics in Graph Theory* (L. W. Beineke and R. J. Wilson, eds.), Academic Press.

P. J. Cameron, J.-M. Goethals, and J. J. Seidel (1978), The Krein condition, spherical designs, Norton algebras and permutation groups, *Proc. Kon. Ned. Akad. v. Wetensch.* **81**, 196–206.

P. J. Cameron and J. H. van Lint (1991), *Designs, Graphs, Codes and their links*, London Math. Soc. Student Texts **22**, Cambridge University Press.

P. J. Cameron and J. H. van Lint (1982), On the partial geometry $pg(6,6,2)$, *J. Combinatorial Theory* (A) **32**, 252–255.

L. C. Chang (1959), The uniqueness and nonuniqueness of triangular association schemes, *Sci. Record Peking Math.* **3**, 604–613.

F. De Clerck and H. Van Maldeghem (1995), Some classes of rank 2 geometries. In F. Buekenhout (editor) *Handbook of Incidence geometry, Buildings and Foundations*, North-Holland.

F. De Clerck (2000), Partial and semipartial geometries: an update, Combinatorics 2000 (Gaeta, Italy).

W. S. Connor (1958), The uniqueness of the triangular association scheme, *Ann. Math. Stat.* **29**, 262–266.

P. Delsarte (1973), An algebraic approach to the association schemes of coding theory, *Philips Res. Repts. Suppl.* **10**.

P. Delsarte, J.-M. Goethals and J. J. Seidel (1977), Spherical codes and designs, *Geometriae Dedicata* **6**, 363–388.

A. M. Duval (1988), A Directed Graph Version of Strongly Regular Graphs, *J. Combinatorial Theory (A)* **47**, 71–100.

A. Gewirtz (1969), The uniqueness of $g(2,2,10,56)$, *Trans. New York Acad. Sci.* **31**, 656–675.

C. D. Godsil and B. D. McKay (1979), Graphs with Regular Neighborhoods, *Combinatorial Mathematics VII*, 127–140, Springer.

J.-M. Goethals and J. J. Seidel (1970), Strongly regular graphs derived from combinatorial designs, *Canad. J. Math.* **22**, 597–614.

D. G. Higman (1975), Invariant relations, coherent configurations and generalized polygons, in: *Combinatorics* (M. Hall, Jr. and J. H. van Lint, eds.), D. Reidel.

[281] D. G. Higman and C. C. Sims (1968), A simple group of order 44,352,000, *Math. Z.* **105**, 110–113.

A. J. Hoffman (1960), On the uniqueness of the triangular association scheme, *Ann. Math. Stat.* **31**, 492–497.

X. Hubaut (1975), Strongly regular graphs, *Discrete Math.* **13**, 357–381.

T. H. Koornwinder (1976), A note on the absolute bound for systems of lines, *Proc. Kon. Ned. Akad. v. Wetensch.* **79**, 152–153.

J. H. van Lint (1983), Partial geometries, *Proc. Int. Congress of Math.*, Warsaw.

J. H. van Lint and A. Schrijver (1981), Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica* **1**, 63–73.

J. H. van Lint and J. J. Seidel (1969), Equilateral point sets in elliptic geometry, *Proc. Kon. Ned. Akad. v. Wetensch.* **69**, 335–348.

A. Neumaier (1979), Strongly regular graphs with smallest eigenvalue $-m$, *Archiv der Mathematik* **33**, 392–400.

A. Neumaier (1980), New inequalities for the parameters of an association scheme, in: *Combinatorics and Graph Theory*, Lecture Notes in Math. **885**, Springer-Verlag.

S. E. Payne and J. A. Thas (1984), *Finite Generalized Quadrangles*, Pitman.

[282] R. M. Wilson (1973/74), Nonisomorphic Steiner triple systems, *Math. Z.* **135**, 303–313.

# 第 22 章 正交拉丁方

两个拉丁方 $L_1: R\times C\to S$ 和 $L_2: R\times C\to T$(有相同的行集和列集)，当对每个有序对 $(s, t)\in S\times T$，存在一个唯一的腔 $(x, y)\in R\times C$ 使得

$$L_1(x,y)=s \quad 和 \quad L_2(x,y)=t$$

时，称这两个拉丁方是*正交的*. 用"正交的"这个词也许不太好，因为在数学中它有其他含义，但这个词太常见了以至于现在也没有人尝试改变它.

例如，如图 22.1 所示，设

$$A:=\begin{bmatrix} A & K & Q & J \\ Q & J & A & K \\ J & Q & K & A \\ K & A & J & Q \end{bmatrix},\quad B:=\begin{bmatrix} \spadesuit & \heartsuit & \diamondsuit & \clubsuit \\ \clubsuit & \diamondsuit & \heartsuit & \spadesuit \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \\ \diamondsuit & \clubsuit & \spadesuit & \heartsuit \end{bmatrix}$$

图 22.1

这里 $R=C=\{1, 2, 3, 4\}$，$S=\{A, K, Q, J\}$，$T=\{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}$. 将两个方阵叠合，可以看到 $S\times T$ 的每个元素恰出现一次，$A$ 和 $B$ 的正交性显而易见.

$$\begin{bmatrix} A\spadesuit & K\heartsuit & Q\diamondsuit & J\clubsuit \\ Q\clubsuit & J\diamondsuit & A\heartsuit & K\spadesuit \\ J\heartsuit & Q\spadesuit & K\clubsuit & A\diamondsuit \\ K\diamondsuit & A\clubsuit & J\spadesuit & Q\heartsuit \end{bmatrix}$$

正交性不依赖所使用的特殊符号集. 在我们的例子中，将扑克牌的花色换成任意顺序的四个符号，得到的方阵仍与 $A$ 正交. 对 $A$ 的符号我们用拉丁字母；如果对 $B$ 用希腊字母，就会明白为何两个正交拉丁方的叠合通常称为*希腊-拉丁方*.



我们用扑克牌给出的例子与所谓的*欧拉 36 个军官问题*类似. 根据传说，凯瑟琳(Catherine)大帝(欧拉住在她的宫廷)要求欧拉安排来自 6 个不同的团且有 6 种不同军衔的 36 个军官(每个团出 6 个不同军衔的军官)，按 6×6 的阵列，使得每一行和每一列包含每个军衔的军官和每个团的军官. 该问题的一个解要求有一对 6 阶的正交拉丁方.

令人惊奇的是，这个问题无解. 无论凯瑟琳是否问过欧拉，他确实在 1779 年考虑过这个问题并相信没有解. 欧拉有进行巨量计算的能力，但不清楚他是否真地检验过所有的情形. 这一工作由 G. Tarry 在 1900 年系统地做了，如今利用计算机做此事很容易. 一个短的证明(仍涉及应分析的几种情形)由 D. R. Stinson(1984)给出.

欧拉知道对 $n$ 的所有奇数值，以及 $n\equiv 0 \pmod 4$，存在一对 $n$ 阶的正交拉丁方. 对奇数阶 $n$ 的正交拉丁方的例子，设 $G$ 为 $n$ 阶的任意一个群，由

$$L_1(x,y):=xy,\quad L_2(x,y):=x^{-1}y$$

定义行集、列集和符号集为 $G$ 的拉丁方 $L_1$ 和 $L_2$.

不存在阶为 2 的一对正交拉丁方，其理由完全是平凡的. 欧拉说，按照他的意见对 $n=2$，6 的不存在性可推广至 $n=10$，14，18，…，即到 $n\equiv 2(\mathrm{mod}\ 4)$. 在 177 年的时间，这个论断以欧拉猜想著称，直到它突然且完全地被 Bose、Parker 和 Shrikhande 反证. 后面我们将证明他们的定理：除 $n=2$，6 之外，对所有的 $n$，存在一对正交拉丁方.

在许多时候，出现了一个更普遍的问题：我们能找到多个拉丁方的集合，使其中的任何两个正交吗？用 $N(n)$表示最大的整数 $k$，存在 $k$ 个 $n$ 阶拉丁方，它们两两正交. 例如，可以把

284

$$C:=\begin{bmatrix}0&\alpha&\beta&\gamma\\ \alpha&0&\gamma&\beta\\ \beta&\gamma&0&\alpha\\ \gamma&\beta&\alpha&0\end{bmatrix}$$

(克莱因(Klein)四元群的加法表)加到图 22.1 的两个拉丁方中，得到三个两两正交的 4 阶拉丁方；于是 $N(4)\geqslant 3$. 注意，正交性的定义对 $n=1$ 或 0 是平凡的或没有意义，因此 $N(1)=N(0)=\infty$.

这里有一个构造，证明对一个素数的幂 $q$，$N(q)\geqslant q-1$. 所有的行集、列集和符号集都是域$\mathbb{F}_q$ 的元素. 对$\mathbb{F}_q$ 中的每个非零元素 $a$，定义 $L_a(x,\ y):=ax+y$；这 $q-1$ 个拉丁方是两两正交的. 我们都知道，方程组

$$\begin{aligned}ax+by&=s\\cx+dy&=t\end{aligned}$$

当 $ad-bc\neq 0$ 时有唯一解$(x,\ y)$，于是容易知道由线性方程定义的两个拉丁方何时是正交的. 下面是 $q=5$ 时的拉丁方：

$$\begin{bmatrix}0&1&2&3&4\\1&2&3&4&0\\2&3&4&0&1\\3&4&0&1&2\\4&0&1&2&3\end{bmatrix},\quad\begin{bmatrix}0&1&2&3&4\\2&3&4&0&1\\4&0&1&2&3\\1&2&3&4&0\\3&4&0&1&2\end{bmatrix},$$

$$\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\1&2&3&4&0\\4&0&1&2&3\\2&3&4&0&1\end{bmatrix},\quad\begin{bmatrix}0&1&2&3&4\\4&0&1&2&3\\3&4&0&1&2\\2&3&4&0&1\\1&2&3&4&0\end{bmatrix}.$$

**定理 22.1** 对 $n\geqslant 2$，我们有 $1\leqslant N(n)\leqslant n-1$.

285

**证明** 为了记号的方便，可以把 $k$ 个两两正交的拉丁方$\{L_i\}_{i=0}^{k}$的行集、列集和符号集变到$\{1,\ 2,\ \cdots,\ n\}$，而且如果需要，也可以重新命名符号使每个拉丁方的第一行是按顺序的 1，2，…，$n$. 现在考虑第二行第一列的元素

$$L_1(2,1),\quad L_2(2,1),\quad \cdots,\quad L_k(2,1).$$

这些元素中没有一个是 1，因为 1 已出现在第一列中．它们是不同的，因为比如说 $L_i(2,1)=L_j(2,1)=s$，则 $L_i(1,s)=L_j(1,s)=s$ 与 $L_i$ 和 $L_j$ 的正交性矛盾．由此得出上界． ■

从上面给出的有限域的构造和简单的定理，我们有

$$N(q)=q-1\quad 如果 q 为一个素数的幂. \tag{22.1}$$

现在，我们想证明拉丁方两两正交的概念等价于读者在前一章中已见到的东西！如果我们首先注意到成为一个拉丁方的性质本身可用正交性的术语描述，定理的断言会更显而易见．例如，一个 5 阶的方阵是拉丁方，当且仅当它与两个方阵

$$\begin{bmatrix}0&0&0&0&0\\1&1&1&1&1\\2&2&2&2&2\\3&3&3&3&3\\4&4&4&4&4\end{bmatrix}\quad 和 \quad \begin{bmatrix}0&1&2&3&4\\0&1&2&3&4\\0&1&2&3&4\\0&1&2&3&4\\0&1&2&3&4\end{bmatrix}$$

正交．

**定理 22.2** *$k$ 个两两正交的 $n$ 阶拉丁方的集合存在，当且仅当存在一个 $(n, k+2)$-网．*

**证明** 假设 $L_i: R\times C\to S_i(1\leqslant i\leqslant k)$ 是两两正交的拉丁方．设 $\mathcal{P}=R\times C$ 是 $n^2$ 个腔的集．粗略地说，在每个方阵中，我们取行、列及"相等的符号"线为线．更正式些，设

$$\mathcal{A}_1=\{\{(x,b):b\in C\}:x\in R\},$$
$$\mathcal{A}_2=\{\{(a,y):a\in R\}:y\in C\},$$
$$\mathcal{A}_{i+2}=\{\{(x,y):L_i(x,y)=c\}:c\in S_i\},\quad 1\leqslant i\leqslant k,$$

286

并设 $\mathcal{B}=\bigcup_{i=1}^{k+2}\mathcal{A}_i$．由拉丁方和正交的定义得 $(\mathcal{P},\mathcal{B})$ 是一个 $(n, k+2)$-网．

给定一个 $(n, k+2)$-网 $(\mathcal{P},\mathcal{B})$，这里 $\mathcal{B}=\bigcup_{i=1}^{k+2}\mathcal{A}_i$ 是 $\mathcal{B}$ 划分为平行类，在 $\mathcal{A}_{i+2}$ 中通过声明 $L_i(A, B)$ 是包含 $A$ 和 $B$ 的交的点的唯一直线定义 $L_i: \mathcal{A}_1\times\mathcal{A}_2\to\mathcal{A}_{i+2}$．像通常那样，我们把验证这些方阵是拉丁方和正交性的细节留给读者． ■

**推论** *$N(n)=n-1$ 当且仅当存在 $n$ 阶的射影（或仿射）平面．*

在一种非常不精确的意义上，$N(n)$ 的值告诉我们离能得到的 $n$ 阶射影平面的存在性多近．但对这个函数我们知道得少之又少．除素数的幂之外我们只知道 $n=6$ 时 $N(n)$ 的值．

**问题 22A** (i)考虑一个 $(n, n)$-网的图的补，并证明 $N(n)\geqslant n-2$ 蕴涵 $N(n)=n-1$．

(ii)利用问题 21F 的结果证明，如果 $n>4$，则 $N(n)\geqslant n-3$ 蕴涵 $N(n)=n-1$．

**定理 22.3** (i) $N(nm)\geqslant\min\{N(n), N(m)\}$．

*(ii)如果 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ 表示 $n$ 分解成素数的幂，则*

$$N(n)\geqslant\min_{1\leqslant i\leqslant r}(p_i^{e_i}-1).$$

**证明** 部分(ii)由部分(i)和(22.1)利用归纳法得到．

为了证明部分(i)，首先我们以自然的方式定义一个类克罗内克积：给定 $L_i: R_i\times C_i\to S_i$，

$i=1, 2$，由

$$(L_1 \otimes L_2)((x_1,x_2),(y_1,y_2)) := (L_1(x_1,y_1), L_2(x_2,y_2))$$

定义

287

$$L_1 \otimes L_2 : (R_1 \times R_2) \times (C_1 \times C_2) \to (S_1 \times S_2).$$

直接验证如果 $\{A_i\}_{i=1}^k$ 是两两正交的 $n$ 阶拉丁方且 $\{B_i\}_{i=1}^k$ 是两两正交的 $m$ 阶拉丁方，则 $\{A_i \otimes B_i\}_{i=1}^k$ 是两两正交的 $nm$ 阶拉丁方. 我们把这个任务留给读者，但建议你读下去而不要厌烦. ■

定理 22.3 以 MacNeish 定理著称. MacNeish 在 1922 年猜想定理 22.3(ii)中的等号成立. 这蕴涵欧拉猜想. 但这种类型的组合问题罕有如此简单的答案.

当借助 4 阶的 21 个点射影平面作出三个 21 阶拉丁方时，MacNeish 猜想首次在 $n=21$ 被证明不正确；见下面的例 22.1. 这是*合成方法*的一个例子，它也提供了欧拉猜想的第一个反例($n=22$). 第一对 10 阶的正交拉丁方由 Parker 用*差方法*发现. 我们先讨论合成方法，对大的 $n$ 值，它们被证明更有用.

对正交拉丁方的集合，Bose、Parker 和 Shrikhande 给出了多种构造. 我们选择用拟群的术语描述两个基本且优美的构造. 回忆一下，*拟群*是一个行集、列集和符号集都是 $X$ 的拉丁方. 当对所有的 $x \in X$，$L(x, x)=x$ 时，拟群 $L$ 是*幂等的*. 例如，如果 $X$ 是 $q$ 阶的有限域 $\mathbb{F}_q$，则

$$L_a(x,y) := ax + (1-a)y$$

定义一个幂等拟群 $L_a$，其中 $a \neq 0, 1$. 这种形式的任意两个拉丁方是正交的.

**问题 22B** 对一个素数的幂 $q \geq 4$，构造两个 $q$ 阶的行集和列集都等于$\mathbb{F}_q$ 的拉丁方 $A$，$S$，使得 $A$ 与其转置和 $S$ 正交，且 $S$ 是对称的. 此外，如果 $q$ 是奇数，则保证 $S$ 是幂等的；如果 $q$ 为偶数，则保证 $S$ 是幂幺的，即 $S$ 的对角线上的元素为常数.

假设在具有线集$\mathcal{A}$的一个点集 $X$ 上有一个线性空间，见第 19 章. 此外，假设对$\mathcal{A}$中的每条线 $A$，我们在集 $A$ 上有 $k$ 个两两正交的幂等拟群 $L_1^A$，$L_2^A$，…，$L_k^A$. 通过对每个 $i=1, 2, \cdots, k$，断言 $L_i(x, x) := x (x \in X)$，且对不同的 $x$，$y \in X$，$L_i(x, y) := L_i^A(x, y)$，这里 $A$ 是$\mathcal{A}$中既包含 $x$ 又包含 $y$ 的唯一一条线，可以在整个集合 $X$ 上构造 $k$ 个两两正交的幂等拟群 $L_1$，$L_2$，…，$L_k$. 检验 $L_1$，$L_2$，…，$L_k$ 是拉丁方且它们正交就很容易了. 例如，给定 $i$，$j$，$s$ 和 $t$，$s \neq t$，一个腔$(x, y)$，对$(x, y)$，

288

$$L_i(x,y) = s \quad \text{和} \quad L_j(x,y) = t$$

存在，$x$，$y$ 可能在包含 $s$ 和 $t$ 的线 $B$ 上找到，因为 $L_i^B$ 和 $L_j^B$ 正交.

**定理 22.4** *对 $n$-集 $X$ 上的具有线集$\mathcal{A}$的每个线性空间，我们有*

$$N(n) \geq \min_{A \in \mathcal{A}} \{N(|A|) - 1\}.$$

**证明** 设 $k$ 是所示的最小值. 这意味着在每个 $A \in \mathcal{A}$ 上，我们有至多 $k+1$ 个两两正交的拟群. 我们描述怎样在每个 $A$ 上获得 $k$ 个两两正交的幂等拟群. 那么由上面的构造得出 $N(n) \geq k$.

一般地，设 $H_1$，$H_2$，…，$H_{k+1}$ 是一个 $m$-集 $B$ 上的两两正交的拟群. 任选 $b \in B$. 有 $m$ 个腔$(x, y)$，对于它们 $H_{k+1}(x, y)=b$，$x$ 在每行中且 $y$ 在每列中. 比如说，同时排列所有拉丁

方的列，使得这些腔位于第 $k+1$ 个拉丁方的对角线上. 正交性蕴涵对每个 $i\leqslant k$，所有 $m$ 个符号出现在第 $i$ 个拉丁方的对角线上. 最后，我们独立地排列前 $k$ 个拉丁方中的符号，使得得到的拉丁方是幂等的. ■

**定理 22.5** 如果$\mathcal{A}$是一个 $n$-集 $X$ 上的线性空间的线的集合，$\mathcal{B}\subseteq\mathcal{A}$是两两不相交的线的集合，则

$$N(n)\geqslant\min(\{N(|A|)-1:A\in\mathcal{A}\setminus\mathcal{B}\}\cup\{N(|B|):B\in\mathcal{B}\}).$$

**证明** 设 $k$ 为所示的最小值. 如我们在上一个定理的证明中所看到的，在$\mathcal{A}/\mathcal{B}$中的每个 $A$ 上有 $k$ 个两两正交的幂等拟群 $L_i^A$. 如有必要，我们给$\mathcal{B}$添上一些单元素集使得$\mathcal{B}$变成 $X$ 的一个划分. 在每个 $B\in\mathcal{B}$上，我们有 $k$ 个两两正交的拟群 $L_i^B$(不必是幂等的). 对每个 $i=1,2,\cdots,k$，通过断言 $L_i(x,x):=L_i^B(x,x)$，这里 $B$ 是$\mathcal{B}$中包含 $x$ 的唯一成员，以及对不同的 $x$，$y$，$L_i(x,y)=L_i^A(x,y)$，这里 $A$ 是$\mathcal{A}$中(无论在不在$\mathcal{B}$中)既包含 $x$ 又包含 $y$ 的唯一的线，我们在整个集合 $X$ 上定义 $L_1$，$L_2$，$\cdots$，$L_k$. 拟群 $L_i$ 是正交的(这个容易的细节留给读者)且因此$N(n)\geqslant k$. ■

[289]

**例 22.1** 设 $n=21$ 并考虑有 21 条规模为 5 的直线的 4 阶射影平面. 定理 22.4 蕴涵 $N(21)\geqslant 3$，这说明 MacNeish 猜想不正确. 删去不共线的三个点. 我们得到一个线性空间，该空间有 18 个点以及规模为 5，4，3 的线；规模为 3 的三条线是两两不交的. 定理 22.5 蕴涵 $N(18)\geqslant 2$，这证明欧拉猜想不正确.

**例 22.2** 为了明白欧拉猜想的错误程度，对 $n\equiv 2(\mathrm{mod}\ 4)$我们考虑另外两个例子. 从阶为 8 的射影平面删去三个不共线的点得到 70 个点的一个线性空间，该空间有规模为 9，8 和 7(两两不交)的线. 定理 22.5 显示 $N(70)\geqslant 6$. 可以从$\mathbb{F}_8$构造的平面上找到 7 个点(甚至 10 个点，见问题 19I)，使得没有三个点共线，删去这些点产生了一个能用于定理 22.4 的线性空间，给出 $N(66)\geqslant 5$.

不用横截设计下面的构造将很难描述. 横截设计提供了一种紧凑的且在概念上方便的语言，用这种语言处理两两正交的拉丁方的集合.（它们也提供了线性空间的一个大族，这些空间对其他组合设计甚至更多的正交拉丁方的构造是有用的.）TD$(n,k)$可以定义为一个$(n,k)$-网的关联结构的对偶，即一个$(n,k,k-1)$-部分几何. 因此有 $nk$ 个点和 $n^2$ 个区组(当讨论横截设计时，我们用“区组”而不用“线”.)每个点在 $n$ 个区组中，每个区组包含 $k$ 个点. $nk$ 个点落入规模为 $n$ 的 $k$ 个等价类(称为群，这会引起混淆)，使得在同一个群中的两个点不被包含在一个区组中，同时在不同群中的两个点恰好属于一个区组. 特别地，每个区组恰好包含来自每个群的一个点. 我们需要如此频繁地引用群，于是把它们合并到一个记号中并论及横截设计$(X,\mathcal{G},\mathcal{A})$，这里的三个坐标分别是点集、群集和区组集. $(X,\mathcal{G}\cup\mathcal{A})$是一个区组规模为 $k$ 和 $n$ 的线性空间.

[290]

**例 22.3** 这里是 TD(2，3)：

群：$\{a_1,a_2\}$，$\{b_1,b_2\}$，$\{c_1,c_2\}$

区组：$\{a_1,b_1,c_1\}$，$\{a_1,b_2,c_2\}$，$\{a_2,b_1,c_2\}$，$\{a_2,b_2,c_1\}$.

按照定理 22.2，TD$(n,k+2)$的存在性等价于 $k$ 个两两正交的拉丁方的存在性. 下面通过快速地描述从 TD$(n,k+2)$得到拉丁方来看一下它们之间的联系：把群编号为$\{G_1,G_2,\cdots,G_{k+2}\}$，通过声明 $L_i\{x,y\}$是 $G_{i+2}$与包含 $x$ 和 $y$ 的区组的交的点，定义 $L_i:G_1\times G_2\rightarrow G_{i+2}$.

$TD(n, k)$称为可分解的，如果区组的集$\mathcal{A}$能划分成 $n$ 个平行类$\mathcal{A}_1$，$\mathcal{A}_2$，…，$\mathcal{A}_n$，即每个$\mathcal{A}_i$ 是一个规模为$k$ 的 $n$ 个区组的集合，这些区组划分点集 $X$. 从 $TD(n, k)(X, \mathcal{G}, \mathcal{A})$，我们总能通过删去一个群 $G_0=\{x_1, x_2, \cdots, x_n\}$的 $n$ 个点来构造一个可分解的 $TD(k-1)$，删去的结果是恰从每个区组移去一个点；对每个 $i$，$x_i$ 已被移去的区组在 $TD(n, k-1)$的点集 $X\setminus G_0$ 上构成一个平行类.（反之，一个可分解的 $TD(n, k-1)$可以扩展为 $TD(n, k)$.）

**定理 22.6** 若 $0\leqslant u\leqslant t$，则

$$N(mt+u)\geqslant \min\{N(m),N(m+1),N(t)-1,N(u)\}.$$

**证明** 设 $k$ 是上式的右端加 2. 这意味着横截设计 $TD(m, k)$，$TD(m+1, k)$，$TD(t, k+1)$ 和 $TD(u, k)$存在；为了证明该定理，我们必须构造 $TD(mt+u, k)$.

由于这个构造相当专业，我们首先描述从 $TD(t, k)$和各种 $TD(m, k)$构造 $TD(mt, k)$. 291 这是定理中 $u=0$ 的退化情形，其构造不需要 $TD(m+1, k)$或$TD(t, k+1)$，因此再次证明定理 22.3(i).

设$(X, \mathcal{G}, \mathcal{A})$是一个 $TD(t, k)$. 对每个 $x\in X$，联系 $m$ 个新元素的集合$M_x$ 使得任意两个集合$M_x$ 不相交. 对 $S\subseteq X$，设 $M_S:=\bigcup_{x\in S}M_x$.

我们在规模为 $kmt$ 的点集$M_X$ 上构造一个群为$\{M_G: G\in\mathcal{G}\}$的 $TD(mt, k)$，每个群的规模为 $mt$；区组$\mathcal{B}$如下得到. 对每个 $A\in\mathcal{A}$，选择区组$\mathcal{B}_A$ 使得

$$(M_A,\{M_x: x\in A\},\mathcal{B}_A)$$

是 $TD(m, k)$，再设$\mathcal{B}=\bigcup_{A\in\mathcal{A}}\mathcal{B}_A$. 验证是直接的.

为了返回到一般的情形，回想 $TD(t, k+1)$的存在性蕴涵可分解的 $TD(t, k)$的存在性. 于是我们有一个 $TD(t, k)(X, \mathcal{G}, \mathcal{A})$，这里 $\mathcal{A}$可划分为平行类$\mathcal{A}_1$，$\mathcal{A}_2$，…，$\mathcal{A}_t$. 我们用一种方式处理前 $u$ 个平行类的区组，用另一种方式处理$\mathcal{B}:=\bigcup_{i=u+1}^{t}\mathcal{A}_i$ 中的区组.

设$(U, \mathcal{H}, \mathcal{C})$是一个 $TD(u, k)$. 我们还需要 $U$ 分成 $u$ 个$k$-子集$\{K_1, K_2, \cdots, K_u\}$的一个划分；每个子集恰由来自每个集合 $H\in\mathcal{H}$的一个点组成，但不要求这些 $k$-子集是$\mathcal{C}$的区组.

设$\mathcal{G}=\{G_1, G_2, \cdots, G_k\}$和$\mathcal{H}=\{H_1, H_2, \cdots, H_k\}$是群的标号. 我们构造一个带有点集 $Y:=M_X\cup U$ 和群

$$\mathcal{J}:=\{M_{G_1}\cup H_1,M_{G_2}\cup H_2,\cdots,M_{G_k}\cup H_k\}$$

的 $TD(mt+u, k)$. 区组如下得到. 如前述一样，对每个区组 $B\in\mathcal{B}$，设

$$(M_B,\{M_x: x\in B\},\mathcal{D}_B)$$

是一个 $TD(m\,k)$. 对每个区组 $A\in CalA_i$，设

$$(M_A\cup K_i,\{(M_A\cap M_{G_j})\cup(K_i\cap H_j): j=1,2,\cdots,k\},D_A)$$

是一个 $TD(m+1, k)$，其中 $K_i$ 作为区组出现，又设$\mathcal{D}'_A$表示剩下的$(m+1)^2-1$ 个区组. 那么我们断言$(Y, \mathcal{J}, \mathcal{E})$是要求的 $TD(mt+u, k)$，这里

292

$$\mathcal{E}:=\mathcal{C}\cup\Big(\bigcup_{B\in\mathcal{B}}\mathcal{D}_B\Big)\cup\Big(\bigcup_{A\in\mathcal{A}_1\cup\cdots\cup\mathcal{A}_u}\mathcal{D}'_A\Big).$$

验证需要考虑几种情形. ■

**例 22.4** 在定理 22.6 中取 $m=3$，我们看到

$$\text{当 } 0 \leqslant u \leqslant t \text{ 时}, N(3t+u) \geqslant 2; N(t) \geqslant 3 \text{ 且 } N(u) \geqslant 2. \tag{22.2}$$

可以取$(t, u)=(5, 3)$，$(7, 1)$，$(7, 5)$和$(9, 3)$，发现对$n=18$，22，26和30，$N(n)\geqslant 2$.

**定理 22.7** 对所有的$n\neq 2$，6，$N(n)\geqslant 2$.

**证明** 我们只需考虑$n\equiv 2 \pmod 4$. 对$n=10$，14，见下面的例22.6和例22.7. 对$n=18$，22，26和30，见上面的例22.4. 现在我们假设$n\geqslant 34$.

$$n-1, n-3, n-5, n-7, n-9, n-11$$

中的一个数能被3整除，但不能被9整除，因此可以写成$n=3t+u$，这里$u=1$，3，5，7，9或11且$t$不能被3整除. 因为$n$是偶数，$t$是奇数，由定理22.3(ii)知$N(t)\geqslant 4$. $n\geqslant 34$的一个结论是$t\geqslant 11$，于是$0\leqslant u\leqslant t$，且由(22.2)得$N(n)\geqslant 2$. ■

**定理 22.8** 当$n\to\infty$时，$N(n)\to\infty$.

**证明** 设$x$为正整数. 我们断言，当

$$n \geqslant 2\Big(\prod_{p\leqslant x} p\Big)^{2x+1} \tag{22.3}$$

时，$N(n)\geqslant x-1$，(22.3)中的乘积扩展到$\leqslant x$的所有素数$p$.

给定满足(22.3)的$n$，设$m$已选定(中国剩余定理)使得$0\leqslant m\leqslant \Big(\prod_{p\leqslant x} p\Big)^{x}$，且对所有的素数$p\leqslant x$，

$$m \equiv \begin{cases} -1 \pmod{p^x} & \text{如果 } p \text{ 整除 } n, \\ 0 \pmod{p^x} & \text{如果 } p \text{ 不整除 } n. \end{cases}$$

然后选择一个整数$t\equiv 1\Big(\bmod \prod_{p\leqslant x} p\Big)$使得

$$0 \leqslant u := n - mt < \Big(\prod_{p\leqslant x} p\Big)^{x+1}.$$

定理剩下的部分由下面的问题22C提供. ■ [293]

**问题 22C** 如上选择$m$，$t$和$u$，证明$u\leqslant t$且定理22.3(ii)蕴涵$N(mt+u)\geqslant x-1$.

* * *

在第19章中，我们已见过由所谓的差方法做出的构造. 这里我们用这个想法构造拉丁方. 用正交阵列来描述我们的构造是很方便的. $OA(n, k)$是一个$k\times n^2$阵列(或者在这里我们更愿意将其看成高度为$k$的$n^2$个列向量的集合，因为列的次序是不重要的)，其项取自$n$个符号的集合$S$，因此对任意不同的$i$，$j$，$1\leqslant i$，$j\leqslant k$，以及$S$中的任意两个符号$s$，$t$，有唯一的一列，它的第$i$个坐标是$s$且第$j$个坐标是$t$. 这推广了在第17章中引入的$OA(n, 3)$.

这不过是正交性的另一个等价刻画，存在一个$OA(n, k+2)$等价于存在$k$个两两正交的拉丁方. 例如，为了从拉丁方$L_1$，$L_2$，…，$L_k$得到阵列，不失一般性，假设行集、列集和符号集都是$S$并取所有的列

$$[i, j, L_1(i,j), L_2(i,j), \cdots, L_k(i,j)]^{\mathrm{T}}, \quad i, j \in S.$$

$$\begin{bmatrix} x & x & x & y & y & y & z & z & z \\ x & y & z & x & y & z & x & y & z \\ x & y & z & z & x & y & y & z & x \\ x & y & z & y & z & x & z & x & y \end{bmatrix}$$

图 22.2

从图22.2中的$OA(3, 4)$，读者应能很快地写出两个正交拉丁方(当然，$OA(3, 4)$的任意两行

可用于“调整”拉丁方.）

**例 22.5** 下面的$\mathbb{Z}_{15}$的元素的矩阵由 Schellenberg，Van Rees and Vanstone(1978)借助计算机发现：

294

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 0 & 2 & 5 & 7 & 9 & 12 & 4 & 1 & 14 & 11 & 3 & 6 & 8 & 10 & 13 \\ 0 & 6 & 3 & 14 & 10 & 7 & 13 & 4 & 11 & 2 & 8 & 5 & 1 & 12 & 9 \\ 0 & 10 & 6 & 1 & 11 & 2 & 7 & 12 & 3 & 8 & 13 & 4 & 14 & 9 & 5 \end{bmatrix}.$$

它有以下性质：对任意两行，这两行的坐标的差包含$\mathbb{Z}_{15}$的所有元素，每个元素的重数是 1. 通过取这些列由$\mathbb{Z}_{15}$的元素所做的所有平移，我们得到一个 $OA(15, 5)$. 因此可以构造三个 15 阶的两两正交的拉丁方. 但 $OA(15, 5)$是可分解的：对任意一列的 15 个平移，在每个坐标，所有的符号出现一次. 正如横截设计一样，可以加上新的一行得到 $OA(15, 6)$，并因此得到四个 15 阶的两两正交的拉丁方. 不知道是否有 $N(15)\geqslant 5$.

上面矩阵的最后三行是下面所说的$\mathbb{Z}_{15}$的两两正交的正交态射.

在 1960 年，Johnson、Dulmage 和 Mendelsohn 利用群$\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_3$ 并借助计算机，用这种方法证明 $N(12)\geqslant 5$. 12 阶的循环群没有用处，见下面的定理 22.9.

**例 22.6** 我们描述一个构造并证明

$$N(m)\geqslant 2\Rightarrow N(3m+1)\geqslant 2.$$

设 $G$ 是 $2m+1$ 阶的交换群(也称为阿贝尔群)，又设 $M$ 为 $G$ 中的对$\{i, -i\}(i\neq 0)$的一个代表系. 这就是 $|M|=m$ 且 $G=\{0\}\cup M\cup -M$. 对每个 $i\in M$，引入一个新符号$\infty_i$ 并取 $S:=G\cup\{\infty_i : i\in M\}$作为 $OA(3m+1, 4)$的符号集.

考虑从

$$\left\{\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}\right\}\cup\left\{\begin{bmatrix} \infty_i \\ 0 \\ i \\ -i \end{bmatrix}, \begin{bmatrix} 0 \\ \infty_i \\ -i \\ i \end{bmatrix}, \begin{bmatrix} i \\ -i \\ \infty_i \\ 0 \end{bmatrix}, \begin{bmatrix} -i \\ i \\ 0 \\ \infty_i \end{bmatrix} : i\in M\right\}$$

295

得到的所有列向量，方法是在$\infty$固定的约定下，即$\infty_i+g=\infty_i$，由 $G$ 的元素平移它们. 这给出$(4m+1)(2m+1)$列. 把 $OA(m, 4)$的 $m^2$ 个列添加到这些列上以得到 $OA(3m+1, 4)$.

在 $m=3$ 的情形更为明显，我们用符号集$\mathbb{Z}_7\cup\{x, y, z\}$和 $M=\{1, 2, 3\}$. 取下面 13 列的 7 个平移并邻接到来自图 22.2 的 $OA(3, 4)$上：

$$\begin{bmatrix} 0 & x & 0 & 1 & 6 & y & 0 & 2 & 5 & z & 0 & 3 & 4 \\ 0 & 0 & x & 6 & 1 & 0 & y & 5 & 2 & 0 & z & 4 & 3 \\ 0 & 1 & 6 & x & 0 & 2 & 5 & y & 0 & 3 & 4 & z & 0 \\ 0 & 6 & 1 & 0 & x & 5 & 2 & 0 & y & 4 & 3 & 0 & z \end{bmatrix}.$$

这一构造的验证需要特别考虑符号 $x$，$y$，$z$(我们曾用它们而不用$\infty$)，以及观察到上面的

行中任意两行的差（当两者的坐标在$\mathbb{Z}_7$中时）包含$\mathbb{Z}_7$的所有元素，每个的重数为 1. 得到的拉丁方如下.

$$\begin{bmatrix} 0 & z & 1 & y & 2 & x & 3 & 6 & 5 & 4 \\ 4 & 1 & z & 2 & y & 3 & x & 0 & 6 & 5 \\ x & 5 & 2 & z & 3 & y & 4 & 1 & 0 & 6 \\ 5 & x & 6 & 3 & z & 4 & y & 2 & 1 & 0 \\ y & 6 & x & 0 & 4 & z & 5 & 3 & 2 & 1 \\ 6 & y & 0 & x & 1 & 5 & z & 4 & 3 & 2 \\ z & 0 & y & 1 & x & 2 & 6 & 5 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & x & y & z \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & z & x & y \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 & y & z & x \end{bmatrix} \quad \begin{bmatrix} 0 & 4 & x & 5 & y & 6 & z & 1 & 2 & 3 \\ z & 1 & 5 & x & 6 & y & 0 & 2 & 3 & 4 \\ 1 & z & 2 & 6 & x & 0 & y & 3 & 4 & 5 \\ y & 2 & z & 3 & 0 & x & 1 & 4 & 5 & 6 \\ 2 & y & 3 & z & 4 & 1 & x & 5 & 6 & 0 \\ x & 3 & y & 4 & z & 5 & 2 & 6 & 0 & 1 \\ 3 & x & 4 & y & 5 & z & 6 & 0 & 1 & 2 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 & x & y & z \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 & y & z & x \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 & z & x & y \end{bmatrix}$$

**例 22.7** 我们描述在符号$\mathbb{Z}_{11} \cup \{x, y, z\}$上的一个$OA(14, 4)$. 取下面 17 列经$\mathbb{Z}_{11}$的元素的 11 个平移，并邻接到来自图 22.2 的$OA(3, 4)$上：

$$\begin{bmatrix} 0 & 0 & 6 & 4 & 1 & x & 1 & 4 & 0 & y & 2 & 6 & 0 & z & 8 & 9 & 0 \\ 0 & 1 & 0 & 6 & 4 & 0 & x & 1 & 4 & 0 & y & 2 & 6 & 0 & z & 8 & 9 \\ 0 & 4 & 1 & 0 & 6 & 4 & 0 & x & 1 & 6 & 0 & y & 2 & 9 & 0 & z & 8 \\ 0 & 6 & 4 & 1 & 0 & 1 & 4 & 0 & x & 2 & 6 & 0 & y & 8 & 9 & 0 & z \end{bmatrix}$$

这一构造的验证仍然需要特别考虑符号$x$，$y$，$z$（我们曾用它们而不用$\infty$）；以及观察到上面的行中任意两行的差（当两者的坐标在$\mathbb{Z}_{11}$中时）包含$\mathbb{Z}_{11}$的所有元素，每个的重数为 1. [296]

**问题 22D** 证明$k$个两两正交的幂等拟群的存在性等价于 TD$(n, k+2)$的存在性，在 TD$(n, k+2)$中可以找到区组的一个平行类.

交换群$G$的*正交态射*是$G$的元素的一个置换$\sigma$，使得

$$x \mapsto \sigma(x) - x$$

也是$G$的一个置换. 读者可以验证：方阵$L(x, y) := \sigma(x) + y$是拉丁方当且仅当$\sigma$是一个置换，且正交于$G$的加法表$A(x, y) := x + y$当且仅当$\sigma$是一个正交态射.

注意，如果$A$有任何一个正交伴侣，则有一个正交态射：在一个正交伴侣包含一个给定符号的位置上，在每一行和每一列恰有一个腔，且对某个置换$\tau$，形式$(x, \tau(x))(x \in G)$也是如此. 因为这些腔必须包含$A$中的不同符号，所以由$\sigma(x) := x + \tau(x)$定义的映射$\sigma$是一个置换. 依照这个说法，下面的定理证明偶数阶的循环方阵没有正交伴侣，即没有拉丁方与它正交.

**定理 22.9** *如果交换群$G$有一个正交态射，则其阶是奇数或者其西罗（Sylow）2-子群不是循环群.*

**证明** 如果西罗 2-子群是循环的且非平凡，则$G$正好有一个 2 阶元$z$. 如果$G$的所有元素相加，除$z$和 0 外每个元素与其加法逆成对；因此$G$的所有元素之和是$z$. 但是，如果$\sigma$是一个正交态射，则

$$z=\sum_{x\in G}(\sigma(x)-x)=\sum_{x\in G}\sigma(x)-\sum_{x\in G}x=z-z=0,$$

[297] 与 $z$ 的选择矛盾. ■

**注记** 如果 $G$ 是交换群且阶为奇数，则它有仅保持单位元不动的自同构（对一些偶数阶的交换群这也正确），并且是正交态射. 即使 $G$ 不是交换群，也可以定义正交态射（也称为完全映射），如果西罗 2-子群是循环的且非平凡，不存在正交态射的结论仍然正确——见Hall and Paige(1955)，在这本书中，证明对有平凡或非循环西罗 2-子群的可解群，存在完全映射.

* * *

H. B. Mann(1950)观察到，具有 $2t$ 阶子拉丁方的 $4t+1$ 阶的拉丁方没有正交伴侣. 类似地，具有 $2t+1$ 阶子拉丁方的 $4t+2$ 阶的拉丁方没有正交伴侣. 这两个结果是下面定理中(ii)的推论，它也证明在例 22.6 中我们构造的 $12t+10$ 阶的正交拉丁方的对子中，没有一对能扩充为有三个或更多个两两正交拉丁方的集合. 我们把弄清子拉丁方对应子横截设计的问题留给读者.

**定理 22.10** 设$(X, \mathcal{G}, \mathcal{A})$是一个包含子-TD$(m, k)(Y, \mathcal{H}, \mathcal{B})$的 TD$(n, k)$，这里 $m<n$.（这意味着 $Y\subseteq X$，$\mathcal{H}=\{G\cap Y: G\in\mathcal{G}\}$，且$\mathcal{B}\subseteq\mathcal{A}$.）则

(i)$m(k-1)\leqslant n$.

(ii)如果$(X, \mathcal{G}, \mathcal{A})$是可分解的，则

$$m^2\geqslant n\left\lceil\frac{mk-n}{k-1}\right\rceil.$$

**证明** 选取一个点 $x_0\in X\setminus Y$. 比如说 $x_0$ 属于 $G_0\in\mathcal{G}$. 对 $m(k-1)$个点 $y\in Y\setminus G_0$ 的每一个，存在满足$\{x_0, y\}\subseteq A_y$ 的唯一区组 $A_y\in\mathcal{A}$. 包含 $Y$ 中两个点的一个区组一定属于$\mathcal{B}$（且不能包含 $x_0$），于是有 $m(k-1)$个区组是不相同的. 这个数不能超过 $x_0$ 上的区组总数，这个总数是 $n$.

[298] 假设$(X, \mathcal{G}, \mathcal{A})$是可分解的且$\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_n\}$是$\mathcal{A}$分成平行类的一个划分. 设 $s_i$ 表示含于 $Y$ 中的$\mathcal{A}_i$ 的区组数，$t_i$ 表示与 $Y$ 正好交于一个点的$\mathcal{A}_i$ 的区组数. 那么

$$ks_i+t_i=|Y|=mk \quad 和 \quad s_i+t_i\leqslant n,$$

由此得出$(k-1)s_i\geqslant mk-n$，或等价地

$$s_i\geqslant\left\lceil\frac{mk-n}{k-1}\right\rceil.$$

从 $m^2=|\mathcal{B}|=\sum_{i=1}^{n}s_i$ 得到(ii). ■

**问题 22E** 证明 $N(24)\geqslant 3$ 且 $N(33)\geqslant 3$.

**问题 22F** 假设我们有 $c-1$ 个两两正交的 $k$ 阶拉丁方，则有一个 $OA(k, c+1)$，其表示如下：

$$\begin{bmatrix}1 & 1 & \cdots & 1 & 2 & 2 & \cdots & 2 & \cdots & k & k & \cdots & k\\ 1 & 2 & \cdots & k & & & & & & & & & \\ \vdots & & & & & & A_1 & & & & A_{k-1} & & \\ 1 & 2 & \cdots & k & & & & & & & & & \end{bmatrix},$$

这里每个矩阵 $A_i$ 的每一行是 1，2，…，$k$ 的一个置换. 设 $A$ 是由矩阵 $A_i$ 构成的 $c\times k(k-1)$ 矩阵. 利用这个矩阵及问题 19U 中的矩阵 $S$ 证明下面的定理.

**定理** 如果存在一个对称的$(v, k, 1)$-设计，则 $N(v)\geqslant N(k)$.

**问题 22G** 推广定理 22.6 如下.

**定理** 如果 $0\leqslant u\leqslant t$，$0\leqslant v\leqslant t$，则

$$N(mt+u+v)\geqslant \min\{N(m),N(m+1),N(m+2),N(t)-2,N(u),N(v)\}.$$

**问题 22H** 证明 $N(21)\geqslant 4$.

**问题 22I** 证明 $N(51)\geqslant 4$. 299

**问题 22J** 假设由给出的例子已证明对 $a\leqslant n\leqslant 7a+3$，$N(n)\geqslant 3$. 证明对 $7a\leqslant n\leqslant 7^2a$，$N(n)\geqslant 3$；并对 $n\geqslant a$ 得出 $N(n)\geqslant 3$ 的结论.

## 评注

一般来说，术语“相互正交的拉丁方”及其首字母缩写“MOLS”比“两两正交的拉丁方”更常见.

我们在第 1 章的评注里已提到欧拉. 欧拉 1782 年的论文标题是“A new type of magic square”，他注意到来自一对正交拉丁方的特殊幻方. 作为一个例子，在图 22.1 中把 $A$ 和 $B$ 的符号集分别改成{4，3，2，1}和{12，8，4，0}，用加而不是叠合以得到

$$\begin{bmatrix} 16 & 11 & 6 & 1 \\ 2 & 5 & 12 & 15 \\ 9 & 14 & 3 & 8 \\ 7 & 4 & 13 & 10 \end{bmatrix}.$$

这个矩阵每条线上的和是 34.（一般地，拉丁方的性质并不蕴涵对角元之和等于“幻方数”，但我们的例子是特别好的拉丁方：对角线、四个角以及许多其他四个项的和等于 34.）

在图 22.1 中，本书的作者知道“$A$”既用作一个矩阵的名字又用作同一矩阵的一个项. 我们只是检查一下读者是否聚精会神.

正交拉丁方通常以正交阵列的形式出现，它在实验设计的统计理论中非常重要.

1922 年 MacNeish 的论文实际上包括欧拉猜想的一个错误的证明.

R. C. Bose(1938)观察到正交拉丁方和有限射影平面之间的联系.

E. H. Moore(1896)预见了正交拉丁方的许多结果，正如 R. D. Baker 向我们指出的. 可是，在 Moore 的论文中找不到拉丁方一词；因此很长时间没有人注意他的结果. 他的论文中包含定理 22.3 和定理 22.4 的特殊情形(虽然形式完全不同)和阶为素数幂的射影平面的描述，因此如果他知道 MacNeish 猜想，就会证明这个猜想不正确. 300

定理 22.6 是 Wilson(1974)的构造的一个特殊情形，Wilson 的构造在几个方面依次被推广，见 T. Beth，D. Jungnickel and H. Lenz(1986).

利用类似于问题 22J 的方法，本书的第二作者证明对 $n\geqslant 47$，$N(n)\geqslant 3$. 现在已知对 $n>10$，$N(n)\geqslant 3$. 对近来多种 $n$ 的下界 $N(n)$，见 Colbourn and Dinitz(1996).

定理 22.8 属于 Chowla，Erdös and Straus(1960). 他们证明得更多：对充分大的 $n$，$N(n)\geqslant n^{1/91}$. 他们的结果是数论的且基于 Bose-Parker-Shrikhande 构造. 他们的结果多次被改进，目前最好的结果是 T. Beth(1983)的. 这似乎离真理甚远. 很可能，比如说对所有的 $n$，或者对除去 $n$ 的有限多个值，有 $N(n)\geqslant n/10$，但从目前的情况来看，这极难证明.

## 参考文献


T. Beth (1983), Eine Bemerkung zur Abschätzung der Anzahl orthogonaler lateinischer Quadrate mittels Siebverfahren, *Abh. Math. Sem. Hamburg* **53**, 284–288.

T. Beth, D. Jungnickel, and H. Lenz (1986), *Design Theory*, Bibliographisches Institut.

R. C. Bose (1938), On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares, *Sanhkya* **3**, 323–338.

R. C. Bose, S. S. Shrikhande, and E. T. Parker (1960), Further results in the construction of mutually orthogonal Latin squares and the falsity of a conjecture of Euler, *Canad. J. Math.* **12**, 189–203.

S. Chowla, P. Erdős, and E. G. Straus (1960), On the maximal number of pairwise orthogonal Latin squares of a given order, *Canad. J. Math.* **12**, 204–208.

C. J. Colbourn and J. H. Dinitz, editors (1996), *The CRC Handbook of Combinatorial Designs*, CRC Press. [301]

A. L. Dulmage, D. Johnson, and N. S. Mendelsohn (1961), Orthomorphisms of groups and orthogonal Latin squares, *Canadian J. Math.* **13**, 356–372.

M. Hall and L. J. Paige (1955), Complete mappings of finite groups, *Pacific J. Math.* **5**, 541–549.

H. F. MacNeish (1922), Euler squares, *Ann. Math.* **23**, 221–227.

H. B. Mann (1950), On orthogonal Latin squares, *Bull. Amer. Math. Soc.* **50**, 249–257.

E. H. Moore (1896), Tactical memoranda I–III, *Amer. J. Math.* **18**, 264-303.

P. J. Schellenberg, G. M. J. Van Rees, and S. A. Vanstone (1978), Four pairwise orthogonal Latin squares of order 15, *Ars Comb.* **6**, 141–150.

D. R. Stinson (1984), Nonexistence of a Pair of Orthogonal Latin Squares of Order Six, *J. Combinatorial Theory* (A) **36**, 373–376.

R. M. Wilson (1974), Concerning the number of mutually orthogonal Latin squares, *Discrete Math.* **9**, 181–198. [302]

# 第23章 射影几何和组合几何

组合几何是一个对子$(X, \mathcal{F})$，这里$X$是一个点集，$\mathcal{F}$是$X$的被称为平坦面的子集之族，使得

(1)$\mathcal{F}$在(两两)交运算之下是闭的.

(2)在偏序集$\mathcal{F}$中没有无穷链.

(3)$\mathcal{F}$包含空集、所有的单元素集$\{x\}(x\in X)$，以及集合$X$自身.

(4)对任意平坦面$E\in\mathcal{F}$，$E\neq X$，在$\mathcal{F}$中覆盖$E$的平坦面划分其余的点.

这里，$F$在$\mathcal{F}$中覆盖$E$是指$E$，$F\in\mathcal{F}$，$E\subsetneq F$，但$E\subsetneq G\subsetneq F$对任意$G\in\mathcal{F}$不成立. 这后一个性质学过几何学的读者应该是熟悉的：包含一个给定点的直线划分其余的点；包含一条给定直线的平面划分其余的点.

组合几何的一个平凡例子是由一个有限集$X$和$X$的所有子集作为平坦面的几何. 这是$X$上的布尔代数.

注意，(1)和(2)蕴涵在任意相交之下，$\mathcal{F}$是闭的.

**例 23.1** 点集$X$上的每个线性空间(如在第19章引入的)，当我们取$\varnothing$、所有的单元素集$\{\{x\}: x\in X\}$、所有的线和$X$自身作为平坦面时，给出点集$X$上的一个组合几何. 事实上，给定点上的线划分其余的点，这是两个点唯一地确定一条线的另一种说法.

**例 23.2** 点集$X$上的每个施泰纳系$S(t, k, v)$，当我们取基数$<t$的所有子集、所有区组和$X$作为平坦面时，就给出$X$上的一个组合几何. 为了由这一构造得到一个几何，不需要所有的区组有相同的规模，只要每个$t$-子集包含在唯一一个区组中就足够了.（见问题19R，在那里我们称之为广义施泰纳系.）

303

**例 23.3** 设$V$为域$\mathbb{F}$上的一个$n$维向量空间. $V$的仿射子空间，是指空集或在加法群中$V$的一个(正常的，即线性的)子空间的陪集(或平移). 例如，对$a$，$b\in\mathbb{F}$，子集$\{(x, y): y=ax+b\}$是$\mathbb{F}^2$的一个仿射子空间. 集合$V$与所有的仿射子空间构成的组合几何称为仿射几何$AG_n(\mathbb{F})$. 我们把$AG_n(\mathbb{F}_q)$写成$AG_n(q)$，$n=2$的情况已在第19章中引入.

**例 23.4** 比$AG_n(\mathbb{F})$更为基本的射影几何$PG_n(\mathbb{F})$，定义起来有些棘手. 设$V$是域$\mathbb{F}$上的一个$(n+1)$维向量空间. $PG_n(\mathbb{F})$的点集$X$由$V$的所有的1维(线性)子空间构成. 例如，如果$\mathbb{F}$是有$q$个元素的域$\mathbb{F}_q$，则$PG_n(\mathbb{F}_q)$的射影点的数目是

$$\frac{q^{n+1}-1}{q-1}=q^n+\cdots+q^2+q+1.$$

对$V$的每个线性子空间$W$，我们联合一个平坦面$F_W$，它由包含在$W$中的$V$的所有1维子空间构成，取$\mathcal{F}$为所有这样的平坦面$F_W$的集合. 我们把$PG_n(\mathbb{F}_q)$写成$PG_n(q)$，$n=2$的情形已在第19章中引入.

射影几何$PG_n(\mathbb{F})$也可作为$\mathbb{F}$的除环(没有乘法的交换性质)定义，见 Crawley and Dilworth(1973).

设$Y$是组合几何$(X, \mathcal{F})$的$X$的任意子集，设

$$\mathcal{E}:=\{F\cap Y: F\in \mathcal{F}\}.$$

则$(Y, \mathcal{E})$也是一个组合几何，称为 $Y$ 上的子几何. 例如，$AG_n(\mathbb{F})$是 $PG_n(\mathbb{F})$的子几何.

304

$AG_n(\mathbb{F})$的点集到 $PG_n(\mathbb{F})$的点集有一个标准的嵌入：对一个 $n$ 维向量空间中的每一个向量 $\boldsymbol{x}$，联合一个 1 维向量子空间，该子空间是由$(\boldsymbol{x}, 1)$在 $n+1$ 维空间 $V\times\mathbb{F}$ 中张成的. 其象是由所有不包含在超平面 $V\times\boldsymbol{0}$ 中的射影点构成的.

当组合几何的平坦集$\mathcal{F}$按包含关系排序时，有一些重要性质.

**格** $L$ 是具有如下性质的偏序集：任意有限子集 $S\subseteq L$ 有一个**盈**(也称为交或最大下界)，即 $L$ 中的一个元素 $b$，使得

$$\forall_{a\in S}[b\leqslant a] \quad 和 \quad \forall_{a\in S}[c\leqslant a]\Rightarrow c\leqslant b,$$

以及一个**不足**(也称为并或最小上界)，即 $L$ 中的一个元素 $b$，使得

$$\forall_{a\in S}[b\geqslant a] \quad 和 \quad \forall_{a\in S}[c\geqslant a]\Rightarrow c\geqslant b.$$

两个元素的集合 $S=\{x, y\}$的盈和不足分别用 $x\wedge y$ 和 $x\vee y$ 表示. 容易看出$\wedge$和$\vee$是交换的、结合的、幂等的二元运算；此外，如果所有的两个元素的子集有盈和不足，则任意有限子集有盈和不足.

我们考虑的格具有不存在无穷链的性质. 这样的格有一个(唯一的)最小元素(用 $0_L$ 表示)，因为不存在无穷链的条件允许我们找到一个极小元素 $m$，而且任意极小元素是最小的，这是因为如果 $m\not\leqslant a$，则 $m\wedge a$ 小于 $m$. 类似地，有一个唯一的最大元素 $1_L$.

对一个偏序集的元素 $a$ 和 $b$，当 $a>b$ 且没有元素 $c$ 使得$a>c>b$ 时，我们说 $a$ **覆盖** $b$ 并且写作 $a\gtrdot b$. 例如，$U$ 和 $W$ 是一个向量空间的线性子空间，当 $U\supseteq W$ 且 $\dim(U)=\dim(W)+1$ 时，$U\gtrdot W$. 回忆一个偏序集 $P$ 的链是 $P$ 的一个全序子集. 于是一个有限链可看成序列$a_0<a_1<\cdots<a_n$. 有最小元素 $0_L$ 的格 $L$ 的**点**是覆盖 $0_L$ 的元素.

**几何格**是没有无穷链的格 $L$；且使得

305

(1)$L$ 是**原子的**，即 $L$ 的每个元素是 $L$ 的点的不足(并).

(2)$L$ 是**半模的**，即如果 $a$ 和 $b$ 不同且在 $L$ 中都覆盖 $c$，则 $a\vee b$ 既覆盖 $a$ 又覆盖 $b$.

**定理 23.1** *按包含关系排序的组合几何的平坦面的集是几何格. 反之，给定点集为 $X$ 的几何格 $L$，则$(X, \{F_y: y\in L\})$是一个组合几何，这里*

$$F_y:=\{x\in X: x\leqslant y\}.$$

**证明** 因为一个组合几何的平坦面的集$\mathcal{F}$在交之下是封闭的，平坦面的偏序集是一个原子格(两个平坦面的盈是它们的交；两个平坦面的不足是包含这两个平坦面的所有平坦面的交). 在一个组合几何中，假设平坦面 $F_1$ 和 $F_2$ 覆盖平坦面 $E$. 设 $x$ 是 $F_1/F_2$ 中的一个点. 在$\mathcal{F}$中有一个平坦面 $G_2$ 覆盖 $F_2$ 并且包含点 $x$. $G_2$ 包含 $F_1$，因为否则 $E\subsetneq F_1\cap G_2\subsetneq F_1$. 但由对称的论证，存在覆盖 $F_1$ 且包含 $F_1$ 和 $F_2$ 的一个平坦面$G_1$. 不足 $F_1\vee F_2$ 必定既包含在$G_1$ 中又包含在 $G_2$ 中. 因为 $G_i$ 覆盖 $F_i$，所以 $F_1\vee F_2=G_1=G_2$.

设 $L$ 为一个几何格，定义平坦面 $F_y$ 为 $L$ 的点集 $X$ 的子集，如在定理的陈述中那样. 显然，空集、任意单元素集和 $X$ 都是平坦面($y$ 分别取 $0_L L$ 的一个点、或 $1_L$). 因为 $x\leqslant y$ 且 $x\leqslant z$，当且仅当 $x\leqslant y\wedge z$，我们有 $F_y\cap F_z=F_{y\wedge z}$；于是$\mathcal{F}:=\{F_y: y\in L\}$在交之下是封闭的. 不

在给定的平坦面 $F_y$ 上的点 $x$ 不能在覆盖 $F_y$ 的两个平坦面中，因此剩下的仅仅是证明覆盖 $F_y$ 的某个平坦面包含 $x$. 我们通过证明 $F_{x\vee y}$覆盖 $F_y$ 完成定理的证明.

这等价于证明在 $L$ 中 $x\not\leqslant y$ 且 $x$ 是 $L$ 的一个点时，$x\vee y \gtrdot y$. 选择一条最大链

$$0_L \lessdot y_1 \lessdot y_2 \lessdot \cdots \lessdot y_k = y.$$

因为 $x$ 和 $y_1$ 覆盖 $0_L$，所以 $x\vee y_1$ 覆盖 $y_1$. 因为 $x\vee y_1$ 和 $y_2$ 覆盖 $y_1$，所以 $x\vee y_2$覆盖 $y_2$(显然 $x\vee y_1\vee y_2=x\vee y_2$). 归纳地，可以得到 $x\vee y_k$ 覆盖 $y_k$. ■

在某种意义上，几何格和组合几何之间的差异与关联结构和一个集合的子集族之间的差异是一样的. 关联结构和格更为抽象，在特定的情形(例如，在讨论对偶和区间时)一定要避免混淆，但在许多论证中，我们更喜欢用集和子集的语言和记号. 306

例如，对一个偏序集的元素 $a$ 和 $b$，区间$[a, b]$定义为$[a, b]:=\{x: a\leqslant x\leqslant b\}$. 在一个格中，任意区间仍然是一个格. 读者应验证：一个几何格的任意区间仍然是一个几何格. 用组合几何的语言叙述它们对应的事实有些不便.

根据定理 23.1(更精确一些，在定理的证明中描述的对应)，把组合几何和几何格的记号和语言混用(尽管有时会引起混淆)常常是方便的. 例如，可以用同样的符号 $PG_n(\mathbb{F})$表示组合几何及对应的一个向量空间的子空间的格.

**问题 23A** (i)作为一个偏序集，对某 $m\leqslant n$，$PG_n(\mathbb{F})$的任意一个区间同构于 $PG_m(\mathbb{F})$. (ii)$PG_n(\mathbb{F})$同构于其对偶偏序集(这里序是反的).

**例 23.5** 划分格 $\Pi_n$，它的元素是一个 $n$-集 $X$ 的所有划分，提供了几何格的另一个族，且因此给出组合几何. 划分按细化排序；$\mathcal{A}$是$\mathcal{B}$的一个细化，如果$\mathcal{B}$的每个区组是$\mathcal{A}$的区组的并. 因此最小元素(最细的划分)是所有的单元素集$\{\{x\}: x\in X\}$且最大元素是$\{X\}$，最小元素和最大元素构成单一的区组. 立刻可以证明一个划分覆盖另一个划分，如果前者是由后者的两个区组结合而成. 点由规模为 2 的单一区组和 $n-2$ 个单元素集构成的划分.

例如，$\Pi_4$ 有 15 个元素：

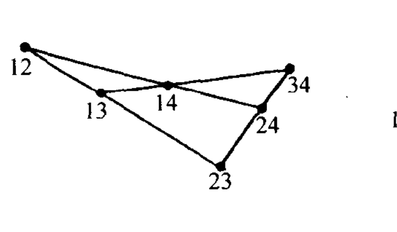
$$\{1234\}$$
$$\{123,4\},\{124,3\},\{134,2\},\{234,1\},\{12,34\},\{13,24\},\{14,23\}$$
$$\{12,3,4\},\{13,2,4\},\{14,2,3\},\{23,1,4\},\{24,1,3\},\{34,1,2\}$$
$$\{1,2,3,4\}$$

307

为了简化记号，作为一个例子，我们把$\{\{1, 2, 3\}, 4\}$写成$\{123, 4\}$.

**例 23.6** $\Pi_n$ 的点与 $K_n$ 的边是一一对应. 给定 $n$ 个顶点上的任意简单图$G$，我们得到一个几何格$L(G)$，它的点与 $G$ 的边集 $E(G)$对应如下. $L$ 的元素是 $V(G)$的所有划分$\mathcal{A}$，那些划分使得由$\mathcal{A}$的每个区组诱导的 $G$ 的子图是连通的. 有这一性质的划分恰是与 $G$ 的边的某个子集对应的点(在 $\Pi_n$ 中)的不足(在 $\Pi_n$ 中). 格 $L(G)$有时称为 $G$ 的收缩的格(见第 33 章).

图 23.1 显示了组合几何 $L(K_4)$和 $L(K_5)$. 例如，$L(K_5)$有 10 个点，在图中标号为 12 的圆点表示点(划分)$\{12, 3, 4, 5\}$. 类型$\{123, 4, 5\}$的划分包含 3 个点且用线段表示；没有显示有两个点的线. (我们注意到 6 个点/7 条线的 $L(K_4)$是由费诺构形删去一个点得到的几何.)



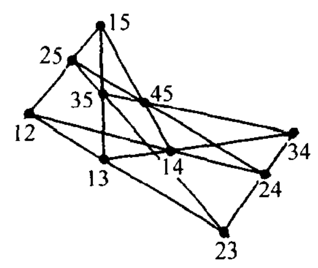




图 23.1

对于一个组合几何的点的子集 $S$，闭包 $\overline{S}$ 是所有包含 $S$ 的平坦面的交. 例如，在一个线性空间中，两个点的集合的闭包是包含这两个点的线. 练习：证明 $S\subseteq\overline{S}$，$A\subseteq B\Rightarrow\overline{A}\subseteq\overline{B}$，且 $\overline{\overline{S}}=\overline{S}$. 有时在平坦面的格中用不足的符号是方便的，注意

308

$$E\vee F:=\overline{E\cup F}.$$

一个子集 $S\subseteq X$，如果对每个 $x\in S$，$x\notin\overline{S\setminus\{x\}}$，则 $S$ 是*独立的*. 在例 23.1 中，一个线性空间中的三个点是独立的，当且仅当它们不被一条线包含；没有四个点是独立的. 在 $PG_n(\mathbb{F})$ 中点的一个集合是独立的，当且仅当代表向量是线性无关的. 在 $AG_n(\mathbb{F})$ 中点的一个集合是独立的，当且仅当代表向量是仿射独立的. 组合几何的一个观点是它们代表"抽象的独立性"的研究.

点集为 $X$ 的组合几何的*秩*是指 $X$ 的独立子集的最大规模. $PG_n(\mathbb{F})$ 和 $AG_n(\mathbb{F})$ 的秩都是 $n+1$. 我们避免用维数一词，如果忘记并用了这个词，它意味着秩减一. 平坦面 $F$ 的独立子集的最大规模是这个平坦面的秩. 秩为 1 的平坦面称为*点*，秩为 2 的平坦面称为*线*，秩为 3 的平坦面称为*平面*. 秩比 rank($X$)小 1 的平坦面称为*超平面*或*上点*(也称*共点*). 有时我们需要用术语*上线*(或*共线*)表示秩等于 rank($X$)$-2$ 的平坦面.

从任意组合几何($X$, $\mathcal{F}$)，可以得到一个线性空间($X$, $\mathcal{L}$)，这里 $\mathcal{L}$ 是所有线(秩为 2 的平坦面)的集合.

在图 23.1 中，任意两点确定一条线，这条线上有两点或三点，只有后者被画在图中. $L(K_5)$中的平面或者有四个点或者有六个点，后者包含四条其上有三个点的线.

下面给出一些简单的事实.

**引理 23.2** (1)*如果 $x\notin\overline{A}$ 但 $x\in\overline{A\cup\{y\}}$，则 $y\in\overline{A\cup\{x\}}$(交换公理).*

*(2)在一个几何中，如果 $S$ 是点的一个独立集且 $x\notin\overline{S}$，则 $\{x\}\cup\{S\}$ 是独立的.*

*(3)如果 $F=\overline{S}$，则对 $S$ 的任意最大的独立集 $A$，$F=\overline{A}$.*

**证明** $F_1:=\overline{A\cup\{x\}}$ 是覆盖 $E:=\overline{A}$ 且包含 $x$ 的平坦面，$F_2:=\overline{A\cup\{y\}}$ 是覆盖 $E$ 且包含 $y$ 的平坦面. 如果 $x\in F_2$，则一定有 $F_1=F_2$，这就证明了(1).

309

如果$\{x\}\cup S$ 不是独立的，存在一个 $y\in S$ 使得 $y\in\overline{(S\cup\{x\})\setminus\{y\}}$. 设 $A:=S\setminus\{y\}$. 因为 $S$ 是独立的，所以 $y\notin\overline{A}$，但这时(1)蕴涵 $x\in\overline{A\cup\{y\}}$，即 $x\in\overline{S}$. 这就证明了(2).

假设 $F=\overline{S}$ 且 $A$ 是 $S$ 的一个独立子集，相对于这个性质 $A$ 是最大的. 如果 $S\not\subseteq\overline{A}$，由(2)可以找到 $S$ 的一个更大的独立子集. 因此 $S\subseteq\overline{A}$，又因为 $F$ 是包含 $S$ 的最小平坦面，所以 $F\subseteq\overline{A}$，这就证明了(3). ■

平坦面 $F$ 的一组基是使得 $\overline{B}=F$ 的一个独立子集 $B\subseteq F$，即 $F$ 的任意极大独立子集. 作为一个练习，读者应检验也可把 $F$ 的一组基定义为极小生成集，即 $F$ 的一个子集 $B$ 使得 $\overline{B}=F$ 且相对于这个性质 $B$ 是极小的.

**问题 23B** 设 $G$ 是一个简单连通图，证明组合几何 $L(G)$ 的基正好是 $G$ 中生成树的边集.

**定理 23.3** 在一个组合几何中，平坦面 $F$ 的所有基有相同的有限基数(称为 $F$ 的秩). 对平坦面 $E$ 和 $F$，有

$$\text{rank}(E)+\text{rank}(F)\geqslant\text{rank}(E\cap F)+\text{rank}(E\vee F).\tag{23.1}$$

**证明** 显然，平坦面没有无穷链的条件迫使所有的独立集是有限的.

如果 $F$ 的所有基有相同的基数不真，选择基满足 $|B_1|>|B_2|$ 的一个有序对 $(B_1, B_2)$，使得在这一限制之下 $|B_2\setminus B_1|$ 尽可能小. 选择 $x\in B_1\setminus B_2$. 那么 $B_1\setminus\{x\}$ 是独立的且有一个闭包不包含 $F$，因此也不包含 $B_2$. 取 $y\in B_2\setminus B_1$ 使得 $y\notin\overline{B_1\setminus\{x\}}$. 由引理 23.2，$(B_1\setminus\{x\})\cup\{y\}$ 是独立的且被 $F$ 的一个基 $B_3$ 包含. 现在我们有满足 $|B_3|>|B_2|$ 的有序对 $(B_3, B_1)$，但 $B_2\setminus B_3$ 是 $B_2\setminus B_1$ 的真子集，矛盾.

为证明定理的第二部分，首先注意到引理 23.2(2)蕴涵平坦面 $E$ 的一组基可扩充为任意包含 $E$ 的平坦面 $E'$ 的一组基.

现在，设 $B$ 是 $E\cap F$ 的一组基，把 $B$ 分别扩充为 $E$ 和 $F$ 的基 $B_1$ 和 $B_2$. 那么包含 $B_1\cup B_2$ 的任何平坦面包含 $E$ 和 $F$，因此包含 $\overline{E\cup F}$；这就是说，$\overline{B_1\cup B_2}=\overline{E\cup F}$，因此 $B_1\cup B_2$ 包含 $\overline{E\cup F}$ 的一组基. 所以 [310]

$$\begin{aligned}\text{rank}(\overline{E\cup F})&\leqslant|B_1\cup B_2|=|B_1|+|B_2|-|B_1\cap B_2|\\&=\text{rank}(E)+\text{rank}(F)-\text{rank}(E\cap F).\end{aligned}$$ ■

不等式(23.1)称为半模律.

注意，定理 23.3 的证明显示，任意一个子集 $S$，$S$ 不必是平坦面，它的所有极大独立子集有相同的基数. 这是对平坦面的陈述的一个推论，这是因为可以把定理 23.4 用于 $S$ 上的子几何.

作为一个练习，确保弄懂如下内容：在一个几何中，设 $E$，$F$ 是满足 $E\subseteq F$ 的平坦面，如果 $\text{rank}(E)=\text{rank}(F)$，则 $E=F$；$F$ 覆盖 $E$ 当且仅当 $\text{rank}(F)=\text{rank}(E)+1$.

对仿射几何 $AG_n(q)$，在秩为 $r$ 的平坦面上，点的数目是 $q^r$. 对射影几何 $PG_n(q)$，在秩为 $r$ 的平坦面上，点的数目是

$$\frac{q^{r+1}-1}{q-1}=q^r+\cdots+q^2+q+1.\tag{23.2}$$

**定理 23.4** 假设在 $v$ 个点上的一个组合几何中，秩为 $i$ 的每个平坦面上恰有 $k_i$ 个点，$i=0, 1, \cdots, n$. 则秩为 $r$ 的平坦面的总数是

$$\prod_{i=0}^{r-1}\frac{(v-k_i)}{(k_r-k_i)}.\tag{23.3}$$

此外，这个点集加上秩为 $r$ 的平坦面的族是一个 2-设计.

**证明** 因为秩为 $r+1$ 的平坦面(包含秩为 $r$ 的一个平坦面)把剩下的 $v-k_r$ 个点划分成规模为 $k_{r+1}-k_r$ 的集合，所以一定恰有 $(v-k_r)/(k_{r+1}-k_r)$ 个这样的平坦面. 对秩为 $r$ 和 $r+1$ 的平坦面 $E$，$F$ 的有序对 $(E, F)$ 进行计数，这里 $E\subseteq F$，再对 $r$ 用归纳法可得到公式(23.3). 注

[311] 意，$k_0=0$且$k_1=1$，因此(23.3)对$r=1$成立.

任意两个点包含在唯一一个秩为2的平坦面中，上面的论证蕴涵秩为2的任意平坦面包含在相同数目的秩为$r$的平坦面中，因此秩为$r$的平坦面给出一个2-设计. ■

$PG_n(q)$的秩为$r$的平坦面的数目称为高斯数，见第24章：等式(23.2)和(23.3)蕴涵$PG_n(q)$的点的数目和超平面的数目相等(也可以通过其他方式认识到这一点)，因此我们有如下的推论.

**推论** *射影几何$PG_n(q)$的点和超平面构成一个满足*

$$v=(q^{n+1}-1)/(q-1),$$
$$k=(q^n-1)/(q-1),$$
$$\lambda=(q^{n-1}-1)/(q-1)$$

*的$(v,k,\lambda)$对称设计.*

**问题 23C** 证明一个关联结构是施泰纳系$S(3,4,2^r)$，其中这个关联结构的点是$AG_r(2)$的点，区组是$AG_r(2)$的平面.

下面的定理属于C. Greene(1970).

**定理 23.5** *在一个有限组合几何中，超平面的数目大于或等于点的数目.*

**证明** 该定理的证明类似于定理19.1的证明. 首先，我们证明，如果一个点$x$不在超平面$H$上，则对秩用归纳法得$x$上的超平面的数目$r_x$大于或等于$H$上的点数$k_H$. 这个断言对秩$\leqslant 2$的几何是平凡的. 由归纳假设，我们知道$H$上的子几何的超平面的数目(即$H$中包含的上线$C$的数目)大于或等于$k_H$，但对每一条这样的上线$C$，我们得到$x$上的一个超平面($C$和$x$的不足).

现在我们重复定理19.1的证明：设$\mathcal{H}$表示超平面的集合. $v:=|X|$，$b:=|\mathcal{H}|$，假设$b\leqslant v$，则

$$1=\sum_{x\in X}\sum_{H\not\ni x}\frac{1}{v(b-r_x)}\geqslant\sum_{H\in\mathcal{H}}\sum_{x\notin H}\frac{1}{b(v-k_H)}=1,$$

[312] 这蕴涵在所有的不等式中，等号一定成立. 因此$v=b$. ■

参看引理23.8之后关于定理23.5中等号成立的“注记”.

在研究$PG_n(\mathbb{F})$时，对向量空间的线性子空间，维数公式

$$\dim(U\cap W)+\dim(U+W)=\dim(U)+\dim(W)$$

起着关键作用. 等价地，对$PG_n(\mathbb{F})$的平坦面$E$和$F$有

$$\operatorname{rank}(E\cap F)+\operatorname{rank}(E\vee F)=\operatorname{rank}(E)+\operatorname{rank}(F). \tag{23.4}$$

这是半模律的一个较强的表述. 事实上，在其中(23.4)成立的组合几何称为是*模的*. 例如，在一个模组合几何中，(23.4)蕴涵包含在一个平面中的两条线一定非平凡地相交(见定理19.1).

**问题 23D** 设$(X,\mathcal{B})$是一个秩为3的有限模组合几何的点和线构成的线性空间. 证明$(X,\mathcal{B})$或者是定理19.1之后定义的拟束，或者是第19章定义的射影平面——这就是说，证明对某整数$n\geqslant 2$，任意两条直线有相同的基数$n+1$且恰有$n^2+n+1$个点.

在第19章我们已引入射影几何$PG_n(\mathbb{F})$并定义了射影平面. 这里是一般的定义：一个*射影几何*是模组合几何，组合几何在其点集不能用两个正常的平坦面之并表示的意义上是*连通的*.

限于篇幅，这里不证明下面的基本结果．其证明见 Veblen and Young(1907)，或 Crawley and Dilworth(1973)．

**定理 23.6** 对某个除环$\mathbb{F}$，每一个秩 $n\geq4$ 的射影几何同构于 $PG_n(\mathbb{F})$．

秩$\leq2$ 的组合几何没有太大意义，但都是模的，而且除了两条点线之外，都是射影几何．由问题 23D，秩为 3 的射影几何等价于在第 19 章引入的射影平面(拟束是不连通的)． 313

根据射影几何，每个组合几何可被合并，这是下一个问题的内容．

**问题 23E** (i)设$(X_1,\mathcal{F}_1)$和$(X_2,\mathcal{F}_2)$是模组合几何，$X_1\cap X_2=\varnothing$，证明$(X_1\cup X_2,\{F_1\cup F_2:F_1\in\mathcal{F}_1,F_2\in\mathcal{F}_2\})$是模组合几何．

(ii)设$(X,\mathcal{F})$是模组合几何，使得 $X$ 是两个平坦面 $X_1$ 和 $X_2$ 的并，这里 $X_1\cap X_2=\varnothing$．设 $\mathcal{F}_i:=\{F\cap X_i:F\in\mathcal{F}\}$，$i=1,2$，证明$(X_i,\mathcal{F}_i)(i=1,2)$是模组合几何且$\mathcal{F}=\{F_1\cup F_2:F_1\in\mathcal{F}_1,F_2\in\mathcal{F}_2\}$．

**问题 23F** 证明一个组合几何$(X,\mathcal{F})$的每个平坦面 $F$ 有一个模补，即存在一平坦面 $E$ 使得 $E\cap F=\varnothing$，$E\vee F=X$ 且 $\mathrm{rank}(E)+\mathrm{rank}(F)=\mathrm{rank}(X)$．

模组合几何的点和线构成的线性空间满足如下称为帕施(Pasch)公理的条件：一条与三角形的两边相交的线也交于第三边．更精确些，假设 $A$，$B$，$C$ 是三条不同的线且 $a$，$b$，$c$ 是与它们关联的三个不同的点，如图 23.2 所示．我们要求包含线 $C$ 上 $a$，$b$ 之外任意一点以及线 $B$ 上 $a$，$c$ 之外任意一点的直线 $L$ 也包含线 $A$ 上 $b$，$c$ 之外的一个点．为了明白这在一个模几何中成立，注意 $L$ 和 $A$ 一定都包含在平面 $P=\overline{\{a,b,c\}}$中，且模方程蕴涵一个平面上的两条线一定非平凡地相交． 314

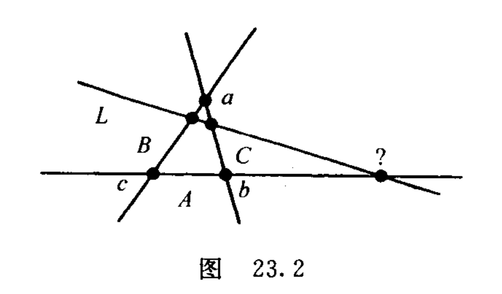



图 23.2

**问题 23G** 考虑其点为一个向量空间 $V$ 的 $k$-维子空间、线为 $V$ 的$(k+1)$-维子空间的关联结构，关联即是包含．证明这个关联结构满足帕施公理．

**定理 23.7** 帕施公理成立的有限线性空间$(X,\mathcal{A})$，是由 $X$ 上的某个模组合几何的点和线构成的．

**证明** 假设帕施公理成立，我们要构造一个组合几何的平坦面，做法如下．说一个子集 $S\subseteq X$ 是平坦面，若对任意线 $L$，

$$|L\cap S|\geq2\text{ 蕴涵 }L\subseteq S.$$

设$\mathcal{F}$表示所有这样的平坦面的集合，它包含空集、所有单元素集、$X$ 以及$\mathcal{A}$中的所有线．检验这个定义蕴涵任意个平坦面的交仍是一个平坦面．

设 $x$ 是不在平坦面 $S$ 上的一个点．设 $T$ 是连结 $x$ 到点 $s\in S$ 的所有线的并．我们断言这个简单的构造产生一个平坦面 $T$，而且 $T$ 覆盖 $S$．

为此，设 $L$ 是包含 $T$ 中两点 $t_1$ 和 $t_2$ 的一条线，我们想证明 $L\subseteq T$．如果 $t_1$ 和 $t_2$ 都属于 $x$ 上的一条线，则 $L$ 是这条直线且因此 $L\subseteq T$．否则，$t_1$ 和 $t_2$ 都在 $S$ 中；则 $L\subseteq T$，因此设 $t_1\notin S$,那么 $t_1$ 和 $t_2$ 分别属于 $x$ 上的不同的线 $M_1$ 和 $M_2$．比如说 $M_i$ 与 $S$ 交于 $s_i$，$i=1,2$，再设 $N$ 是连结 $s_1$ 和 $s_2$ 的线．我们有 $N\subseteq S$，帕施公理保证 $L$ 与 $N$ 交于 $S$ 的某一点 $z$．

考虑另外任意一个点 $t_3 \in L$. 设 $M_3$ 为连结 $x$ 和 $t_3$ 的线. 因为 $M_3$ 与边为 $M_1$, $L$ 和 $N$ 的三角形(顶点为 $z$, $t_1$ 和 $s_1$)的两边相交, 所以它一定与第三边 $N$ 交于 $S$ 的某个点 $s_3$. 那么 $M_3$ 是连结 $x$ 到 $S$ 的点中的一条线, 因此 $t_3 \in T$. 现在我们已证明 $T$ 是一个平坦面.

容易看出 $T$ 覆盖 $S$: 如果 $U$ 是一个平坦面, $S \subsetneq U \subseteq T$. 取 $y \in U \setminus S$. 由构造, 连结 $x$ 和 $y$ 的线是 $x$ 上与 $S$ 相交的一条线; 这条线包含 $U$ 的两个点, 因此被包含在 $U$ 中. 这意味着 $x \in$ 315 $U$, 由此 $T \subseteq U$.

因为任意一点所在的平坦面覆盖一个平坦面 $S$, 所以$(X, \mathcal{F})$是一个组合几何. ($X$ 是有限的假设在这里只用于保证平坦面没有无穷链.)

设 $x$ 为线 $L$ 上的一个点, 又设 $H$ 为任意一个超平面. 因为(如果 $x$ 不在 $H$ 上)$H$ 和 $x$ 的不足一定是 $X$, 所以 $L$ 一定是 $x$ 上与 $H$ 相交的一条线. 这就是说, 任意一条线 $L$ 与任意一个超平面 $H$ 非平凡地相交. 根据下面的引理 23.8, 这蕴涵我们所构建的组合几何是模的. ■

**引理 23.8** 一个组合几何是模的当且仅当它的任意一条线和任意一个超平面非平凡地相交.

**证明** 模律(23.4)表明, 在秩为 $n$ 的几何中秩为 2 的平坦面与秩为 $n-1$ 的平坦面交于秩$\geqslant 1$ 的一个平坦面.

为证明其逆, 我们对秩用归纳法. 假设在一个秩为 $n$ 的组合几何中, 所有的线和超平面非平凡地相交. 假设 $H$ 是一个超平面, 而且存在一条线 $L \subseteq H$ 和秩为 $n-2$ 的平坦面 $C \subseteq H$ 不相交. 那么对任意一个点 $x \notin H$, 超平面 $C \vee \{x\}$ 与线 $L$ 不相交. 因此由归纳法, 任意超平面 $H$ 上的子几何是模的.

于是, 如果存在一对平坦面 $E$ 和 $F$ 提供模律(23.4)的一个反例, 则 $E \vee F$ 等于整个点集 $X$. 设 $H$ 为包含 $E$ 的超平面, 又设 $F' := H \cap F$, 则 $E \vee F' \subseteq H$. 但 $\mathrm{rank}(F') \geqslant \mathrm{rank}(F)-1$, 否则在 $F$ 中 $F'$ 的模补的秩$\geqslant 2$ 且因此包含一条线, 这条线与 $H$ 不相交. 我们看到包含在 $H$ 中的 $E$ 和 $F'$ 提供了(23.4)的一个反例, 这与子几何 $H$ 的模性质矛盾. ■

**注记** 假设一个有限组合几何$(X, \mathcal{F})$的超平面数等于该几何的点数. 那么, 回顾定理 23.5 的证明, 无论何时 $x \notin H$, $r_x = k_H$. 如果在任意一个组合几何中, 把定理 23.5 用于区间$[\{x\}, X]$, 可以得到 $r_x \geqslant l_x$, 这里 $l_x$ 表示包含 $x$ 的线数(因为这些线是几何格$[\{x\}, X]$的点). 对 $x \notin H$, 显然 $l_x \geqslant k_H$, 因为诸线$\{x\} \vee \{y\}$是不同的, 316 这里 $y \in H$. 总之, 定理 23.5 中的等号成立蕴涵当 $x \notin H$ 时, $l_x = k_H$. 这意味着每条线与每个超平面相交, 因此由引理 23.8, $(X, \mathcal{F})$是模的.

说两个三角形$\{a_1, b_1, c_1\}$和$\{a_2, b_2, c_2\}$是从一个点透视的, 如果存在一个点 $p$(透视点)使得$\{p, a_1, a_2\}$共线, $\{p, b_1, b_2\}$共线且$\{p, c_1, c_2\}$共线. 说两个三角形$\{a_1, b_1, c_1\}$和$\{a_2, b_2, c_2\}$是从一条线透视的, 如果存在一条线 $L$(透视线或透视轴)使得$\{L_1, A_1, A_2\}$共点, $\{L, B_1, B_2\}$共点且$\{L, C_1, C_2\}$共点. 这里我们用"三角形"表示三个不共线的点, $A_i$, $B_i$ 和 $C_i$ 表示这个三角形中 $a_i$, $b_i$ 和 $c_i$ 分别对的边. 这就是说, $A_i = \overline{\{b_i, c_i\}}$, $i=1, 2$, 等等.

在图 23.3 中, 两个三角形从点 $p$ 是透视的, 而从直线 $L$ 也是透视的. 用 10 个点和 10 条线图示的这个关联结构, 每条线在三个点上且每个点在三条线上, 称之为德萨格(Desargues)

构形．两个三角形不必位于一个平面上．作为一个关联结构，图 23.1 中的右图与图 23.3 中的图同构(!)；前者容易想象成 3 维的．它可以用多种方式来看，例如，三角形{25，35，45}和{12，13，14}是从点 15 透视的，也是从线{23，24，34}透视的．

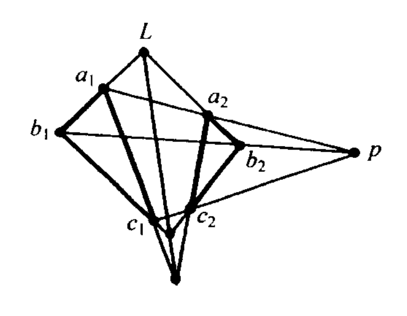


图 23.3

如果选择$(n+1)$维向量空间的一组基，该空间的子空间组成 $PG_n(\mathbb{F})$，则可以用所谓的齐次坐标描述射影点．$\langle x_0, x_1, \cdots, x_n\rangle$是由向量$(x_0, x_1, \cdots, x_n)$生成的一维子空间．

317

射影点$\langle x_0, x_1, \cdots, x_n\rangle$与$\langle y_0, y_1, \cdots, y_n\rangle$相同当且仅当向量$(y_0, y_1, \cdots, y_n)$是$(x_0, x_1, \cdots, x_n)$的非零标量倍数．超平面也可由齐次的$(n+1)$元组描述：$[c_0, c_1, \cdots, c_n]$表示由满足 $c_0x_0+x_1c_1+\cdots+x_nc_n=0$ 的齐次坐标$\langle x_0, x_1, \cdots, x_n\rangle$构成的超平面．

**定理 23.9**(德萨格定理)　在 $PG_n(\mathbb{F})$中，如果两个三角形是从一个点透视的，则它们也是从一条线透视的．

**证明**　设两个三角形$\{a_1, b_1, c_1\}$和$\{a_2, b_2, c_2\}$是从点 $p$ 透视的．为了不在细节上花费太多时间，我们假设 $p$，$a_1$，$b_1$ 和 $c_1$ 中没有三个点共线．再假设所有的点在一个平面上，即我们对 $PG_2(\mathbb{F})$证明该定理．其他情形留给读者．

选择 3-维向量空间的一组基，使得基向量 $\boldsymbol{x}$，$\boldsymbol{y}$，$\boldsymbol{z}$ 分别生成一维子空间 $a_1$，$b_1$，$c_1$．那么 $a_1$，$b_1$ 和 $c_1$ 的齐次坐标分别为$\langle 1, 0, 0\rangle$，$\langle 0, 1, 0\rangle$和$\langle 0, 0, 1\rangle$．设 $p$ 有齐次坐标$\langle \alpha, \beta, \gamma\rangle$，这里所有的坐标不为零．我们把原来的基向量换成 $\alpha\boldsymbol{x}$，$\beta\boldsymbol{y}$ 和 $\gamma\boldsymbol{z}$，则 $a_1$，$b_1$ 和 $c_1$ 仍分别由$\langle 1, 0, 0\rangle$，$\langle 0, 1, 0\rangle$和$\langle 0, 0, 1\rangle$表示，此时 $p$ 的齐次坐标为$\langle 1, 1, 1\rangle$．这会简化我们的计算．

由此得出，对 $\alpha, \beta, \gamma\in\mathbb{F}$，$a_2=\langle \alpha, 1, 1\rangle$，$b_2=\langle 1, \beta, 1\rangle$，$c_2=\langle 1, 1, \gamma\rangle$．连结 $a_1$ 和 $b_1$ 的线是$[0, 0, 1]$，连结 $a_2$ 和 $b_2$ 的线是$[1-\beta, 1-\alpha, \alpha\beta-1]$(验证 $a_2$ 和 $b_2$ 都在这条线上)．在这两条线上的点是$\langle 1-\beta, \alpha-1, 0\rangle$．类似地，可以找到连结 $b_1$ 和 $c_1$ 的线与连结 $b_2$ 和 $c_2$ 的线的交点是$\langle 0, 1-\alpha, \gamma-1\rangle$，连结 $c_1$ 和 $a_1$ 的线与连结 $c_2$ 和 $a_2$ 的线的交点是$\langle \beta-1, 0, 1-\gamma\rangle$．因为这三个交点的坐标是线性相关的，所以它们共线．

(如果我们细心，可以发现这个证明对除环$\mathbb{F}$ 也行得通．)　■

318

**问题 23H**　当$\mathbb{F}$ 是一个(交换的)域时，证明 $PG_n(\mathbb{F})$的线性空间也满足如下的帕普斯(Pappus)定理．设 $a_i$，$b_i$ 和 $c_i$ 是在比如说 $L_i$ 上的共线点，其中 $i=1, 2$．假设 $L_1$ 和 $L_2$ 交于一个点(不是指这六个点之一)．那么线$\overline{\{a_1, b_2\}}$和$\overline{\{a_2, b_1\}}$交于点 $c$，线$\overline{\{b_1, c_2\}}$和$\overline{\{b_2, c_1\}}$交于点 $a$，$\overline{\{a_1, c_2\}}$和$\overline{\{a_2, c_1\}}$交于点 $b$，且三点 $a$，$b$，$c$ 共线．见图 23.4．

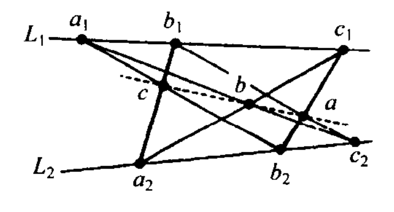


图 23.4

定理 23.9 的陈述成立的射影平面(如果两个三角形从一个点是透视的，则它们从一条线也是透视的)称为德萨格平面．问题 23H 的结论成立的射影平面称为帕普斯平面．限于篇幅，这里不证明进一步的基本结果，见 Crawley and

Dilworth(1973).

**定理 23.10** (i)对某个除环$\mathbb{E}$，秩为 3 的一个射影几何同构于 $PG_2(\mathbb{E})$，当且仅当它是一个德萨格平面.

(ii)对某个域$\mathbb{F}$，秩为 3 的一个射影几何同构于 $PG_2(\mathbb{F})$，当且仅当它是一个帕普斯平面.

定理 23.10 的一个推论是：每个帕普斯平面是德萨格平面. 帕普斯定理蕴涵德萨格定理的一个综合法(即不用坐标)证明，见 D. Pedoe(1963). 我们说每个有限除环是域(韦德伯恩(Wedderburn)定理)，所以每个有限的德萨格平面是帕普斯平面，见 M. Hall, Jr. (1972).

319 下面描述得到非德萨格平面的有限射影平面的一个方法.

设 $G$ 为一个 $n^2$ 阶的交换群，并存在 $n$ 阶的子群 $H_0$，$H_1$，…，$H_n$，它们划分 $G$ 的非零元素，即使得对 $i\neq j$，$H_i\cap H_j=\{0\}$，所以

$$\bigcup_{i=0}^{n} H_i \setminus \{0\} = G \setminus \{0\}.$$

那么，我们断言其点是 $G$ 的元素且线是所有子群 $H_i$ 的所有陪集(平移)的关联结构是一个仿射平面. 一般地，两个子群 $H$ 和 $K$ 的陪集的交或者是空集，或者是 $H\cap K$ 的陪集，所以线至多交于一点. 可以对被覆盖的对子计数以便证明每两个不同的点被一条线包含，这是很简单的，只要注意给定两点 $x$，$y\in G$，陪集 $H_\ell+y$ 包含这两个点，这里 $H_\ell$ 是包含差 $x-y$ 的子群. 以这种方式从群 $G$ 和 $n+1$ 个子群得到的一个仿射平面称为仿射平移平面. 已知为使这样的子群存在，$G$ 一定是基本交换群，见 J. André(1954). 一个仿射平面(如在问题 19K 中)可补足为一个射影平面，由这种方式得到的射影平面是平移平面.

**例 23.7** 这里是$\mathbb{F}_3^4$的非零元素分为 10 个子集 $H_0$，$H_1$，…，$H_9$ 的一个划分.(我们把元素作为串，省略逗号和括号.)

{0000,1000,2000,0100,0200,1100,2200,2100,1200}

{0000,0010,0020,0001,0002,0011,0022,0021,0012}

{0000,1010,2020,0101,0202,1111,2222,2121,1212}

{0000,2010,1020,0201,0102,2211,1122,1221,2112}

{0000,0110,0220,2001,1002,2111,1222,2221,1112}

{0000,0210,0120,1001,2002,1211,2122,1121,2212}

{0000,1110,2220,2101,1202,0211,0122,1021,2012}

{0000,2210,1120,1201,2102,0111,0222,2021,1012}

{0000,2110,1220,2201,1102,1011,2022,0121,0212}

{0000,1210,2120,1101,2202,2011,1022,0221,0112}

320 对应于子群的这个“展形”的仿射平面是德萨格平面.

但是注意前四个子群的元素，可以按另外的方式划分为子群，例如下面的列所示的子群.

| {0000, | {0000, | {0000, | {0000, |
|---|---|---|---|
| 1000,2000, | 0100,0200, | 1100,2200, | 2100,1200, |
| 0010,0020, | 0001,0002, | 0011,0022, | 0021,0012, |
| 1010,2020, | 0101,0202, | 1111,2222, | 2121,1212, |
| 2010,1020} | 0201,0102} | 2211,1122} | 1221,2112} |

上面的例子是下面将描述的构造在 $q=3$ 时的特殊情况. 设 $V$ 是$\mathbb{F}_{q^2}$上的 2 维向量空间且设 $H_0$，$H_1$，…，$H_{q^2}$是$\mathbb{F}_{q^2}$上的 1 维子空间. 如果把 $V$ 看成是$\mathbb{F}_q$ 上的 4 维向量空间，子空间 $H_i$ 在$\mathbb{F}_q$ 上是 2 维的(它们在 $PG_3(q)$中形成线的*展形*；见定理 24.3). 设 $U$ 是$\mathbb{F}_q$ 上除 $H_i$ 之外的任意一个 2 维子空间，则 $U$ 与任意一个 $H_i$ 交于$\{0\}$或$\mathbb{F}_q$ 上的一个一维子空间. 比如说 $U$ 与 $H_0$，$H_1$，…，$H_q$ 中的每一个交于 $q$ 个点，与 $H_{q+1}$，$H_{q+2}$，…，$H_{q^2}$ 只交于零向量. 当 $\alpha$ 遍历$\mathbb{F}_{q^2}$中的非零元素时，考虑$\mathbb{F}_q$-子空间 $\alpha U$；因为乘以$\mathbb{F}_q$ 的非零元保持 $U$ 不动，所以只有$(q^2-1)/(q-1)$个这样的不相同的子空间，比如说是 $U_0$，$U_1$，…，$U_q$. 这 $q+1$ 个子空间 $U_i$ 两两只交于零向量且它们的并是 $H_0\cup H_1\cup\cdots\cup H_q$. 因此

$$U_0, U_1, \cdots, U_q, H_{q+1}, H_{q+2}, \cdots, H_{q^2}$$

是 $V$ 分成 $q^2$ 阶子群的另一种划分.

这里我们不证明由这种构造得到的射影平面不是德萨格平面(对 $q>2$). 见 D. R. Hughes and F. C. Piper(1973)中的定理 10.9. 在例 23.7 中读者可手工找出德萨格定理的反例.

在结束本章之前，我们给出定理 23.6 的困难证明中的重要一步的证明，为此需如下的预备知识.

**命题 23.11** *一个射影几何的任意平坦面上的子几何仍是射影几何.*

**证明** 在一个模射影几何的平坦面上的子几何中，可立刻得到模律成立. 我们必须证明这些子几何是连通的. 为此仅需证明，如果 $H$ 是具有点集 $X$ 的射影几何中的一个超平面，则 $H$ 上的子几何是连通的.

321

如果 $H$ 不连通，$H=E\cup F$，这里 $E$ 和 $F$ 是平坦面. 由(23.4)，$\mathrm{rank}(E)+\mathrm{rank}(F)=n-1$，这里 $n:=\mathrm{rank}(X)$. 设 $E_1$，…，$E_s$ 和 $F_1$，…，$F_t$ 分别是覆盖 $E$ 和 $F$ 的平坦面，它们包含 $H$ 之外的点；每一个族划分 $H$ 之外的点. 假设 $s$，$t$ 都$\geqslant 2$. 由(23.4)，存在 $x_i\in E_i\cap F_i$，$i=1$，2. 又由(23.4)，线$\overline{\{x_1, x_2\}}$与 $H$ 交于某个点 $e\in E$. 那么在 $e$ 和 $x_1$ 的连线上的 $x_2$ 一定包含在 $E_1$ 中，矛盾. 因此 $s$ 和 $t$ 中的一个一定是 1，比如说 $s=1$ 且 $X$ 是不相交的平坦面 $F$ 和 $E_1$ 的并，这与原始的射影几何的连通性矛盾. ■

命题 23.11 的一个推论是，射影几何的每条线至少有三个点(因为有两个点的线是不连通的). 这被用在下面证明的关键之处. 注意，借助于问题 23D，容易看出在一个有限射影几何中所有的线有相同的规模 $n+1$.

**定理 23.12** *德萨格定理对秩$\geqslant 4$ 的任意射影几何成立.*

**证明** 考虑从点 $x$ 是透视的两个三角形$\{a_1, b_1, c_1\}$和$\{a_2, b_2, c_2\}$.

首先假设分别由$\{a_1, b_1, c_1\}$和$\{a_2, b_2, c_2\}$张成的平面 $P_1$ 和 $P_2$ 是不同的. 设 $T:=\overline{\{x, a_1, b_1, c_1\}}$. 线$\overline{\{x, a_1\}}$，$\overline{\{x, b_1\}}$和$\overline{\{x, c_1\}}$分别包含点 $a_2$，$b_2$ 和 $c_2$，故 $P_1$ 和 $P_2$ 被 $T$ 包

含，$T$ 显然有秩 4. 因此由模律，$P_1$ 和 $P_2$ 一定交于一条线 $L$. 我们断言两个原来的三角形从线 $L$ 透视的.

平面 $Q:=\overline{\{p, a_1, b_1\}}$ 包含 $a_2$ 和 $b_2$，因此包含线 $\overline{\{a_1, b_1\}}$ 和 $\overline{\{a_2, b_2\}}$，所以这两条线交于一个点，比如说是 $q$. 点 $q$ 既属于 $P_1$ 又属于 $P_2$，因此 $q\in L$. 类似地，线 $\overline{\{b_i, c_i\}}(i=1, 2)$ 交于 $L$ 上的一个点；线 $\overline{\{a_i, c_i\}}(i=1, 2)$ 交于 $L$ 上的一个点. 因此，两个三角形从 $L$ 是透视的.

[322] 现在假设原来的两个三角形位于平面 $P$ 上. 设 $x_1$ 是不在 $P$ 上的任意一个点且 $x_2$ 是包含 $x_1$ 和 $p$ 的直线上的任意其他点. 线 $\overline{\{x_1, a_1\}}$ 和 $\overline{\{x_2, a_2\}}$ 包含在平面 $\overline{\{p, x_1, a_1\}}$ 中且因此交于一点 $a^*$. 类似地，线 $\overline{\{x_1, b_1\}}$ 和 $\overline{\{x_2, b_2\}}$ 交于一点 $b^*$，线 $\overline{\{x_1, c_1\}}$ 和 $\overline{\{x_2, c_2\}}$ 交于一点 $c^*$. 平面 $P^*:=\overline{\{a^*, b^*, c^*\}}$ 且 $P$ 包含在一个秩为 4 的平坦面中，因此交于一条线 $L:=P\cap P^*$.

三角形 $\{a_1, b_1, c_1\}$ 和 $\{a^*, b^*, c^*\}$ 从点 $x_1$ 是透视的且位于不同的平面上，因此从线 $L$ 是透视的. 类似地，三角形 $\{a_2, b_2, c_2\}$ 和 $\{a^*, b^*, c^*\}$ 从点 $x_2$ 是透视的，因此从线 $L$ 是透视的. 线 $\overline{\{a_1, b_1\}}$ 和 $L$ 的交点与 $\overline{\{a^*, b^*\}}$ 和 $L$ 的交点相同；线 $\overline{\{a_2, b_2\}}$ 和 $L$ 的交点与 $\overline{\{a^*, b^*\}}$ 和 $L$ 的交点相同；因此线 $\overline{\{a_1, b_1\}}$ 和 $\overline{\{a_2, b_2\}}$ 交于 $L$ 上的一点. 类似地，原来的两个三角形的对应"边"交于 $L$ 上的点. 总之，原来的两个三角形从 $L$ 是透视的. ■

**问题 23I** 在划分格 $\Pi_n$ 中确定秩为 $n-k$ 的平坦面的数目.

**问题 23J** 对任意一个区组设计(参数为 $v, k, \lambda, b, r$)，我们定义一条线为包含一对顶点 $x, y$ 的所有区组的交. 证明：

(i)任意两个点在唯一的一条线上.

(ii)如果 $L$ 是一条线，则 $2\leqslant |L|\leqslant\frac{b-\lambda}{r-\lambda}$.

(iii)如果一条线与一个区组交于两点，则它包含在这个区组中.

## 评注

德萨格(Girard Desargues，1593—1662)是建筑师和军事工程师，在关于透视的著作中，他引入了术语对合. 他在法国里昂和巴黎工作. 最后一个著名的希腊几何学家是埃及亚历山大的帕普斯(鼎盛期 320 年)，他的工作要早得多. 射影几何这一数学分支直到 19 世纪才得以发展.

帕施(Moritz Pasch)原来是代数学家，但后来他对非欧几里得几何感兴趣. 27 岁时他作为 [323] 无俸讲师[⊖]来到德国吉森并在这里直至去世(60 年以后). 1893～1894 年他任该地大学的校长.

组合几何的一个起源于二部图的有趣家族称为横截几何；见 Crapo and Rota(1970). 这些几何的独立集是二划分$(X, Y)$的 $X$ 的那些子集，使得它们具有能在 $Y$ 中匹配的性质.

我们已经看到组合几何和几何格的概念是"隐形相关的"，即它们是同一结构的本质上不同的公理系统. Crapo and Rota(1970)给出了更多的隐形相关的形式. 例如，"拟阵"或多或少是与组合几何相同的东西，尽管拟阵论强调的重点有所不同.

⊖ 报酬直接来自学生学费. ——编辑注

由一个有限的射影空间的点和超平面构成的对称设计的一些特征，可在 P. Dembowski (1968)的 2.1 节中找到.

## 参考文献


J. André (1954), Über nicht-Desarguessche Ebenen mit transitiver Translationgruppe, *Math. Zeitschr.* **60**, 156–186.

L. M. Batten (1986), *Combinatorics of Finite Geometries*, Cambridge University Press.

H. Crapo and G.-C. Rota (1970), *Combinatorial Geometries*, MIT Press.

P. Crawley and R. P. Dilworth (1973), *Algebraic Theory of Lattices*, Prentice-Hall.

P. Dembowski (1968), *Finite Geometries*, Springer-Verlag.

C. Greene (1970), A rank inequality for finite geometric lattices, *J. Combinatorial Theory* **9**, 357–364.

M. Hall, Jr. (1972), *The Theory of Groups*, 2nd edn., Chelsea.

D. R. Hughes and F. C. Piper (1973), *Projective Planes*, Springer-Verlag.

D. Pedoe (1963), *An Introduction to Projective Geometry*, Macmillan.

O. Veblen and J. W. Young (1907), *Projective Geometries* (2 vols.), Ginn Co.


324

# 第 24 章　高斯数和 $q$-类似

一个有限集的所有子集的偏序集与一个有限向量空间的所有子空间的偏序集之间有许多类似．这主要是因为它们都是上一章定义的“拟阵设计”的例子．设 $V_n(q)$表示 $q$ 个元素的域$\mathbb{F}_q$ 上的一个 $n$ 维向量空间．我们用术语 $k$-子空间作为 $k$ 维子空间的缩略形式．

下面从计数开始．为了得到 $V_n(q)$的所有子空间的偏序集中的一个最大链（即规模为 $n+1$ 的链，它包含每个可能维数的一个子空间），我们以 0-子空间开始．在已经选择了一个 $i$-子空间 $U_i(1\leqslant i<n)$之后，我们可以选择一个$(i+1)$-子空间 $U_{i+1}$，它以$(q^n-q^i)/(q^{i+1}-q^i)$种方式包含 $U_i$，因为我们能取 $U_i$ 和任意不在 $U_i$ 中的$(q^n-q^i)$个向量之一的生成——但以这种方式任何$(i+1)$-子空间恰出现$(q^{i+1}-q^i)$次．总之，在 $V_n(q)$中子空间的最大链的数目是

$$M(n,q)=\frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)\cdots(q^2-1)(q-1)}{(q-1)^n}.$$

对每个整数 $n$，把 $M(n,\ q)$作为 $q$ 的一个多项式考虑．当变量 $q$ 换成一个素数的幂时，我们得到偏序集 $PG_n(q)$中最大链的数目．当 $q$ 用 1 代替时，我们有 $M(n,\ 1)=n!$，这是在一个 $n$-集合的子集的偏序集中最大链的数目．

325 高斯数$\begin{bmatrix}n\\k\end{bmatrix}_q$ 可以定义为 $V_n(q)$的 $k$-子空间的数目．为强调它们与二项式系数的类似，有些作者称高斯数为*高斯系数*．为了寻找$\begin{bmatrix}n\\k\end{bmatrix}_q$ 的一个表达式，我们对$(U,\ C)$对的数目 $N$ 计数，这里 $U$ 是一个 $k$-子空间且 $C$ 是包含 $U$ 的一个最大链．当然，每个最大链恰包含一个维数为 $k$ 的子空间，于是 $N=M(n,\ q)$．另一方面，通过把包含 $U$ 的 $V_n(q)$的所有子空间的偏序集中的一个最大链附加到 $U$ 的所有子空间的偏序集中的一个最大链上，我们唯一地得到每个这样的最大链，$U$ 中有 $M(k,\ q)$个最大链；包含 $U$ 的 $V_n(q)$中的最大链有 $M(n-k,\ q)$个，这是因为偏序集$\{W:U\subseteq W\subseteq V\}$同构于维数为 $n-k$ 的商空间 $V/U$ 的子集的偏序集．因此

$$\begin{bmatrix}n\\k\end{bmatrix}_q=\frac{M(n,q)}{M(k,q)M(n-k,q)}=\frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

为了某些意图，把$\begin{bmatrix}n\\k\end{bmatrix}_q$ 作为一个变量 $q$ 的多项式考虑比作为一个素数的幂 $q$ 的函数考虑为好．可以由几种方式看出上面的有理函数事实上就是多项式．例如，很容易明白，$x$ 的有理函数对无穷多取整数的 $x$ 是整数，则这个有理函数一定是 $x$ 的多项式．也许*高斯多项式*是比*高斯数*或*高斯系数*更好的一个术语．例如，

$$\begin{bmatrix}6\\3\end{bmatrix}_q=q^9+q^8+2q^7+3q^6+3q^5+3q^4+3q^3+2q^2+q+1.$$

在$\begin{bmatrix}n\\k\end{bmatrix}_q$ 中当 $q$ 被 1 代替时，我们得到$\binom{n}{k}$．这解释了一种倾向的一小部分：关于有限向量空间的结果约化为当 $q$ 由 1 代替时集合的相应结果．当我们试图用“$k$-子空间”代替“$k$-子集”时，可能得到所谓集合上结果的 *$q$-类似*．有时这些替换后的陈述是正确的且其证明与对集合上结果的证明类似．

下面的定理是 Sperner 定理，即定理 6.3 的 $q$-类似. [326]

**定理 24.1** *如果 $\mathcal{A}$ 是一个反链，它在 $V_n(q)$ 的所有子空间的偏序集中，则*

$$|\mathcal{A}| \leqslant \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q.$$

**证明** 设 $\mathcal{A}$ 是一个反链并对 $(U, \mathcal{C})$ 对的数目 $N$ 计数，这里 $U \in \mathcal{A}$ 且 $\mathcal{C}$ 是包含 $U$ 的一个最大链. 每个最大链至多包含 $\mathcal{A}$ 中的一个子空间，因此 $N \leqslant M(n, q)$. 另一方面，在 $\mathcal{A}$ 中每个 $k$-子空间正好位于 $M(k, q)M(n-k, q)$ 个最大链 $\mathcal{C}$ 中. 于是

$$M(n,q) \geqslant N = \sum_{k=0}^{n} c_k M(k,q) M(n-k,q),$$

这里 $c_k$ 是属于 $\mathcal{A}$ 的 $k$ 维子空间的数目. 如果我们相信对所有 $k$ 有 $\begin{bmatrix} n \\ k \end{bmatrix}_q \leqslant \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q$，则以类似于证明定理 6.3 的方式可完成本定理的证明，$\begin{bmatrix} n \\ k \end{bmatrix}_q \leqslant \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q$ 留给读者验证. ■

下面的定理给出作为 $q$ 的多项式系数的 $\begin{bmatrix} n \\ k \end{bmatrix}_q$ 的组合解释，并因此证明它们都是正整数.

**定理 24.2** 设

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{\ell=0}^{k(n-k)} a_\ell q^\ell.$$

*则系数 $a_\ell$ 是 $\ell$ 的分拆数，$\ell$ 的 Ferrers 图适合规模 $k \times (n-k)$ 的方格.*

**证明** 我们可以用 $\mathbb{F}_q$ 上的 $n$ 元组的向量空间 $\mathbb{F}_q^n$ 进行证明. 众所周知，$\mathbb{F}_q^n$ 的每个 $k$-子空间作为 $\mathbb{F}_q$ 上一个 $k \times n$ 矩阵的行空间唯一地出现，该矩阵满足：(i)秩为 $r$，(ii)它是所谓的行约化阶梯形. 这意味着在每一行第一个非零项是 1，首 1 上面的项是 0，第 $i$ 行的首 1 比第 $i-1$ 行的首 1 更靠右端，其中 $i=2, 3, \cdots, k$. [327]

假设第 $i$ 行的首 1 出现在第 $c_i$ 列，其中 $i=1, 2, \cdots, k$. 则 $(n-k+1-c_1, n-k+2-c_2, \cdots, n-1-c_{k-1}, n-c_k)$ 是非负数的一个非增序列，因此当末端的 0 去掉时，对应某个数至多分成 $k$ 部分、每部分的规模至多为 $n-k$ 的一个划分. 反之，这样的划分在阶梯形的一个类中给出首 1 的位置.

例如，在 $n=6$，$k=3$ 的情形，阶梯形有 20 个类；参见图 24.1.

$$\begin{bmatrix} 1&0&0&\bullet&\bullet&\bullet \\ 0&1&0&\bullet&\bullet&\bullet \\ 0&0&1&\bullet&\bullet&\bullet \end{bmatrix} \begin{bmatrix} 1&0&\bullet&0&\bullet&\bullet \\ 0&1&\bullet&0&\bullet&\bullet \\ 0&0&0&1&\bullet&\bullet \end{bmatrix} \begin{bmatrix} 1&0&\bullet&\bullet&0&\bullet \\ 0&1&\bullet&\bullet&0&\bullet \\ 0&0&0&0&1&\bullet \end{bmatrix} \begin{bmatrix} 1&0&\bullet&\bullet&\bullet&0 \\ 0&1&\bullet&\bullet&\bullet&0 \\ 0&0&0&0&0&1 \end{bmatrix} \begin{bmatrix} 1&\bullet&0&0&\bullet&\bullet \\ 0&0&1&0&\bullet&\bullet \\ 0&0&0&1&\bullet&\bullet \end{bmatrix}$$

$$\begin{bmatrix} 1&\bullet&0&\bullet&0&\bullet \\ 0&0&1&\bullet&0&\bullet \\ 0&0&0&0&1&\bullet \end{bmatrix} \begin{bmatrix} 1&\bullet&0&\bullet&\bullet&0 \\ 0&0&1&\bullet&\bullet&0 \\ 0&0&0&0&0&1 \end{bmatrix} \begin{bmatrix} 1&\bullet&\bullet&0&0&\bullet \\ 0&0&0&1&0&\bullet \\ 0&0&0&0&1&\bullet \end{bmatrix} \begin{bmatrix} 1&\bullet&\bullet&0&\bullet&0 \\ 0&0&0&1&\bullet&0 \\ 0&0&0&0&0&1 \end{bmatrix} \begin{bmatrix} 1&\bullet&\bullet&\bullet&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{bmatrix}$$

$$\begin{bmatrix} 0&1&0&0&\bullet&\bullet \\ 0&0&1&0&\bullet&\bullet \\ 0&0&0&1&\bullet&\bullet \end{bmatrix} \begin{bmatrix} 0&1&0&\bullet&0&\bullet \\ 0&0&1&\bullet&0&\bullet \\ 0&0&0&0&1&\bullet \end{bmatrix} \begin{bmatrix} 0&1&0&\bullet&\bullet&0 \\ 0&0&1&\bullet&\bullet&0 \\ 0&0&0&0&0&1 \end{bmatrix} \begin{bmatrix} 0&1&\bullet&0&0&\bullet \\ 0&0&0&1&0&\bullet \\ 0&0&0&0&1&\bullet \end{bmatrix} \begin{bmatrix} 0&1&\bullet&0&\bullet&0 \\ 0&0&0&1&\bullet&0 \\ 0&0&0&0&0&1 \end{bmatrix}$$

$$\begin{bmatrix} 0&1&\bullet&\bullet&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{bmatrix} \begin{bmatrix} 0&0&1&0&0&\bullet \\ 0&0&0&1&0&\bullet \\ 0&0&0&0&1&\bullet \end{bmatrix} \begin{bmatrix} 0&0&1&0&\bullet&0 \\ 0&0&0&1&\bullet&0 \\ 0&0&0&0&0&1 \end{bmatrix} \begin{bmatrix} 0&0&1&\bullet&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{bmatrix} \begin{bmatrix} 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{bmatrix}$$

图 24.1

在图 24.1 的每个矩阵中，当插入列被删去并通过一条竖直的轴反射这些圆点时，圆点的位置描述了一个(≤9 的数的)分拆的 Ferrers 图，这个图可以包含在 3×3 的方格中. 例如，第一行最后一个矩阵表示的类包含 $q^7$ 个阶梯形.

一般地，首 1 在第 $i$ 行出现在 $c_i$ 列的阶梯形的类，对某个 $\ell$，包含 $q^\ell$ 个矩阵，这里 $i=1, 2, \cdots, k$,因为不包含 1 或不需要是 0 的位置可以任意填充$\mathbb{F}_q$ 的元素. 为了精确，

$$\ell = (n-k+1-c_1) + \cdots + (n-1-c_{k-1}) + (n-c_k),$$

因为对每个 $i$，在第 $i$ 行有 $n-(k-i)-c_i$ 个位置可任意填充. 这就是，该类由 $q^\ell$ 个矩阵构成，这里至多分成 $k$ 部分、每部分的规模至多为 $n-k$ 的划分，对应的类事实上是数 $\ell$ 的分拆. 328

于是，若 $a_\ell$ 定义为$\ell$ 的分拆数，$\ell$ 的 Ferrers 图可以包含在 $k\times(n-k)$格子中，我们有一个多项式 $\sum_{\ell=0}^{k(n-k)} a_\ell q^\ell$，当对任意的素数幂 $q$ 计算时，其值与多项式$\begin{bmatrix} n \\ k \end{bmatrix}_q$ 相等，因此这两个多项式相等. ■

注意，当在定理 24.2 的陈述中置 $q=1$ 时，作为一个推论可以得到一个结果：Ferrers 图可以包含在 $k\times(n-k)$个格子中的划分的总数是$\binom{n}{k}$.

**问题 24A** 直接证明这个结果.

接下来，我们对高斯数导出递推式(24.1). 这提供了另一种方式来理解它们是 $q$ 的多项式(比如说，对 $n$ 用归纳法). 取一个超平面 $H$，即 $V_n(q)$的一个$(n-1)$-子空间. 一些 $k$-子空间包含在 $H$ 中(它们的数目是$\begin{bmatrix} n-1 \\ k \end{bmatrix}_q$)，且其余的 $k$-子空间与 $H$ 交于一个$(k-1)$-子空间. $H$ 中的这$\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$ 个$(k-1)$-子空间中每一个包含在 $V$ 的

$$\begin{bmatrix} n-k+1 \\ 1 \end{bmatrix}_q = \frac{q^{n-k+1}-1}{q-1}$$

个 $k$-子空间中，其中，

$$\begin{bmatrix} n-k \\ 1 \end{bmatrix}_q = \frac{q^{n-k}-1}{q-1}$$

个包含在 $H$ 中；而剩下 $q^{n-k}$个不包含在 $H$ 中. 因此

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q. \tag{24.1}$$

**问题 24B** 确定指数 $e_i$(它们可能是 $m$, $n$, $k$，以及 $i$ 的函数)，使得下列等式成立：

$$\begin{bmatrix} n+m \\ k \end{bmatrix}_q = \sum_{i=0}^{k} q^{e_i}\begin{bmatrix} n \\ i \end{bmatrix}_q\begin{bmatrix} m \\ k-i \end{bmatrix}_q.$$

329

(解这个问题的一个途径涉及阶梯形，另一个是用(24.1).)

问题 24B 的等式是二项式系数的等式

$$\binom{n+m}{k} = \sum_{i=0}^{k}\binom{n}{i}\binom{m}{k-i}$$

的一个 $q$-类似. 容斥的 $q$-类似出现在下一章，一个应用见定理 25.2.

(简单的)$t$-设计的 $q$-类似是什么？是 $V_v(q)$ 的 $k$-子空间的一个族 $\mathcal{B}$，使得每个 $t$-子空间恰好包含在 $\mathcal{B}$ 的 $\lambda$ 个成员中．在 1986 年 S. Thomas 描述满足

$$q=2,\quad \lambda=7,\quad t=2,\quad k=3,\quad v\equiv\pm 1 \pmod 6$$

的一个族之前，不知道 $t\geqslant 2$ 时这样的"$q$-$S_\lambda(t,k,v)$"的非平凡的例子．

$t=\lambda=1$ 的情形对向量空间已经是非平凡的．对集合，$S(1,k,v)$ 是一个 $v$-集合分成 $k$-子集的划分，$S(1,k,v)$ 存在当且仅当 $k$ 整除 $v$．

**定理 24.3** *存在 $V_v(q)$ 的 $k$-子空间的一个族，使得每个 1-子空间恰好包含在该族(所谓的 $k$-子空间的展形)的一个成员中，当且仅当 $k$ 整除 $v$.*

**证明** 换言之，我们感兴趣的 $k$-子空间的族是它们中任意的两个交于 0-子空间且它们的并是整个 $v$ 维向量空间．

我们所需的 $k$-子空间的数目是非零向量的总数除以一个 $k$-子空间中非零向量的数目，即 $(q^v-1)/(q^k-1)$．这是一个整数当且仅当 $k$ 整除 $v$．

假设 $v=km$，这里 $m$ 是一个整数．作为 $\mathbb{F}_q$ 上的一个 $v$ 维向量空间，取 $\mathbb{F}_{q^k}$ 上的一个 $m$ 维向量空间 $V$．$V$ 作为 $\mathbb{F}_{q^k}$ 上的向量空间，设 $\mathcal{B}$ 为 $V$ 的 1-子空间的族．(因此有 $q^{k(m-1)}+q^{k(m-2)}+\cdots+q^k+1$ 个族，且每个族中有 $q^k$ 个向量．)现在把 $V$ 作为 $\mathbb{F}_{q^k}$ 的子域 $\mathbb{F}_q$ 上的向量空间，$\mathcal{B}$ 的成员是 $\mathbb{F}_q$ 上的 $k$ 维子空间且提供了所需要的划分． ■ [330]

**问题 24C** 设 $\mathcal{B}$ 是 $V_v(q)$ 中 $k$-子空间的一个展形．设 $\mathcal{A}$ 由 $\mathcal{B}$ 的所有成员的陪集构成．证明 $\mathcal{A}$ 是点集 $V_v(q)$ 上的一个 $S(2,q^k,q^v)$ 的区组集．($v=2k$ 的情形特别有趣，因为我们得到 $q^k$ 阶的仿射平面，从展形得到的平面称为*平移平面*．)

**问题 24D** 证明

$$\sum_{k=0}^{n}(q^n-1)\cdots(q^{n-k+1}-1)q^{\binom{k}{2}}\begin{bmatrix}n\\k\end{bmatrix}_q=q^{n^2}.$$

埃德斯-拉多定理(见定理 6.4)可以用两种(等价的)方式描述．在一种描述中 $m$ 的界是 $\binom{n-1}{k-1}$，在另一种描述中 $m$ 的界是 $\frac{k}{n}\cdot\binom{n}{k}$，这里 $\binom{n}{k}$ 是 $n$-集合的 $k$-子集的总数．

现在考虑一个可能的 $q$-类似．以集 $\mathcal{A}:=\{A_1,A_2,\cdots,A_m\}$ 开始，它们是 $\mathbb{F}_q$ 上的 $n$ 维向量空间 $V(n,q)$ 的 $m$ 个不同的 $k$ 维子空间，满足任意两个 $A_i$ 交于维数 $\geqslant 1$ 的一个子空间．那么可以猜测，如果 $k\leqslant\frac{1}{2}n$，

$$m\leqslant\begin{bmatrix}n-1\\k-1\end{bmatrix}_q\quad\text{或者}\quad m\leqslant\frac{k}{n}\cdot\begin{bmatrix}n\\k\end{bmatrix}_q.$$

在这一情形，两个界是不同的．第一个界强于第二个界．第一个界的一个证明，见 W. N. Hsieh(1975)．这个结果已被 P. Frankl and R. M. Wilson(1986)加强．通过推广定理 6.4 的证明可证明第二个界，这是下一个问题．

**问题 24E** 考虑以上描述的情况．设 $\pi:=(\mathbf{x}_1,\mathbf{x}_2,\cdots,\mathbf{x}_n)$ 取遍 $V(n,q)$ 的所有有序基的集合 $B_n$．我们把 $\pi$ 放在一个圈上．如果 $k$ 个相继向量 $\mathbf{x}_i$(在圈上)的一个序列是 $A_j$ 的基，我们说 $A_j\in\pi$．

(i)证明对一个固定的 $\pi$，有 $|\mathcal{A}\cap\pi|\leqslant k$.

(ii)对一个固定的 $A_j$，对 $\pi\in B_n$ 使得 $A_j\in\pi$ 的基 $\pi$ 的数目计数.

(iii)证明

331

$$m\leqslant\frac{k}{n}\cdot\begin{bmatrix}n\\k\end{bmatrix}_q.$$

## 评注

曾有人建议用记号 $n^{\overset{q}{\cdot}}$ (发音为"$n$ $q$-torial")代替 $M(n, q)$，那么我们有

$$\begin{bmatrix}n\\k\end{bmatrix}_q=\frac{n^{\overset{q}{\cdot}}}{k^{\overset{q}{\cdot}}(n-k)^{\overset{q}{\cdot}}}.$$

注意

$$\lim_{q\to1}n^{\overset{q}{\cdot}}=n^{\overset{1}{\cdot}}\qquad(\text{即 } n!).$$

我们不知是谁首先提出的.

在 1972 年 R. L. Graham、K. Leeb 和 B. L. Rothschild 解决拉姆齐定理的 $q$-类似之前，它是一个长期悬而未决的著名问题.

高斯(Carl Friedrich Gauss，1777—1855)可能是古往今来最伟大的数学家(科学家). 他对数论做出了重大贡献. 他首先研究了今天称为高斯多项式或高斯数的表达式的性质.

## 参考文献


P. Frankl and R. M. Wilson (1986), The Erdős-Ko-Rado theorem for vector spaces, *J. Combinatorial Theory* (A) **43**, 228–236.

R. L. Graham, K. Leeb, B. L. Rothschild (1972), Ramsey's theorem for a class of categories, *Adv. Math.* **8**, 417–433.

R. L. Graham, B. L. Rothschild, and J. Spencer (1980), *Ramsey Theory*, Wiley.

W. N. Hsieh (1975), Intersection theorems for systems of finite vector spaces, *Discrete Math.* **12**, 1–16.

332

S. Thomas (1986), Designs over finite fields, *Geometriae Dedicata* **24**, 237–242.

# 第25章　格和默比乌斯反演

属于组合学基础的一个技巧是偏序集的默比乌斯反演原理. 这个原理可以认为是容斥原理的推广，也可认为是第10章讨论过的数论中带有经典的默比乌斯函数的反演的推广.

设 $P$ 是一个有限偏序集，我们考虑矩阵 $\alpha$，其行和列由 $P$ 的元素标号，即从 $P\times P$ 映射到有理数或复数. 关联代数 $\mathbb{A}(P)$ 由使得 $\alpha(x, y)=0$（除非在 $P$ 中 $x\leqslant y$）的所有矩阵 $\alpha$ 组成. 由矩阵乘法的定义，

$$(\alpha\beta)(x,y) = \sum_{z\in P}\alpha(x,z)\beta(z,y).$$

如果 $\alpha$，$\beta\in\mathbb{A}(P)$，则上面的和需扩展到只在区间 $[x, y]:=\{x\leqslant z\leqslant y\}$ 中的那些 $z$，容易看出 $\mathbb{A}(P)$ 在乘法及加法和标量乘法之下封闭.

$\mathbb{A}(P)$ 的一个元素 $\zeta$（$P$ 的 zeta 函数）在如下的理论中有重要作用，它由

$$\zeta(x,y) = \begin{cases}1 & \text{在 } P \text{ 中 } x\leqslant y,\\ 0 & \text{否则}\end{cases}$$

定义. 我们断言 $\zeta$ 是可逆的，且其逆称为 $P$ 的默比乌斯函数并用 $\mu$ 表示，$\mu$ 是整数且位于 $\mathbb{A}(P)$ 中.

这很容易验证. 等式 $\mu\zeta=I$（恒等元）要求

333

$$\sum_{x\leqslant z\leqslant y}\mu(x,z) = \begin{cases}1 & \text{若 } x=y,\\ 0 & \text{否则},\end{cases} \tag{25.1}$$

这可通过声明如果 $x\not\leqslant y$，$\mu(x, x):=1$，$\mu(x, y):=0$，以及

$$\mu(x,y) := -\sum_{x\leqslant z<y}\mu(x,z) \quad P\text{ 中 } x<y, \tag{25.2}$$

由归纳地定义 $\mu$ 加以保证. 例如，当整数12的所有（正数）因子的格 $P=\{1, 2, 3, 4, 6, 12\}$ 时，

$$\zeta = \begin{bmatrix}1&1&1&1&1&1\\0&1&0&1&1&1\\0&0&1&0&1&1\\0&0&0&1&0&1\\0&0&0&0&1&1\\0&0&0&0&0&1\end{bmatrix},\quad \mu = \begin{bmatrix}1&-1&-1&0&1&0\\0&1&0&-1&-1&1\\0&0&1&0&-1&0\\0&0&0&1&0&-1\\0&0&0&0&1&-1\\0&0&0&0&0&1\end{bmatrix}.$$

$\mu$ 的首行如下计算：

$$\begin{aligned}
&\mu(1,1) = +1,\\
&\mu(1,2) = -\mu(1,1) = -1,\\
&\mu(1,3) = -\mu(1,1) = -1,\\
&\mu(1,4) = -\mu(1,1) - \mu(1,2) = 0,\\
&\mu(1,6) = -\mu(1,1) - \mu(1,2) - \mu(1,3) = +1,\\
&\mu(1,12) = -\mu(1,1) - \mu(1,2) - \mu(1,3) - \mu(1,4) - \mu(1,6) = 0.
\end{aligned}$$

如果我们考虑的是关系 $\zeta\mu=I$，则得到关于 $\mu$ 的一个稍微不同的方程：

$$\sum_{x\leqslant z\leqslant y}\mu(z,y)=\begin{cases}1 & \text{若 } x=y,\\ 0 & \text{否则}.\end{cases} \tag{25.3}$$

334 下面以一种复杂得多的方式来讨论 $\zeta$ 的可逆性. 首先我们说一个有限偏序集总能被一个全序“控制”，这就是，存在一个指标 $P=\{x_1, x_2, \cdots, x_n\}$ 使得在 $P$ 中 $x_i\leqslant x_j$ 蕴涵 $i\leqslant j$.（证明：设 $x$ 为 $P$ 中任意一个最大元素，用归纳给 $P\setminus\{x\}$ 排序，并置 $x$ 在末尾.）相对于 $P$ 的这样一个指标，$\mathbb{A}(P)$中的矩阵是上三角的，zeta 函数在对角线上有 1 且因此行列式为 1，由克拉默(Cramer)公式，它有整数逆. 则 $\zeta^{-1}=\mu$ 位于$\mathbb{A}(P)$中，因为任意一个矩阵(或有限维交换代数的元素)的逆是那个矩阵(或元素)的一个多项式.

等式(25.2)蕴涵着，如果 $x\lessdot y$ 则 $\mu(x, y)=-1$. 注意，如果区间$[x, y]$是一条 $k$-点线，即区间由 $x$, $y$, 以及 $k$ 个两两不可比的元素 $z_1$, $\cdots$, $z_k$ 构成，对每个 $z_i$, $x\lessdot z_i\lessdot y$，则 $\mu(x, y)=k-1$.

在下一个定理中，我们列出一些常见偏序集的默比乌斯函数的值. 定理 25.1 的证明直到本章的末尾才给出，因为我们想先谈及默比乌斯反演的应用. 聪明的和/或刻苦的读者有能力用递归式(25.2)和简单的归纳证明定理 25.1 的若干部分，但我们宁可等到 Weisner 定理(即定理 25.3)出现之后. 这里不证明(v)——见评注.

**定理 25.1** (i)对一个 $n$-集合 $X$ 的所有子集的格，

$$\mu(A,B)=\begin{cases}(-1)^{|B|-|A|} & \text{如果 } A\subseteq B,\\ 0 & \text{否则}.\end{cases}$$

(ii)对整数 $n$ 的所有(正的)因子的格，

$$\mu(a,b)=\begin{cases}(-1)^r & \text{如果}\dfrac{b}{a}\text{是 } r \text{ 个不同素数之积},\\ 0 & \text{否则,即如果 } a\nmid b \text{ 或}\dfrac{b}{a}\text{有平方因子}.\end{cases}$$

(这就是，$\mu(a, b)=\mu\left(\dfrac{b}{a}\right)$，这里后一个 $\mu$ 是(10.8)中单变量的经典函数.)

(iii)对 $q$ 个元素的有限域$\mathbb{F}_q$ 上的一个有限维向量空间 $V$ 的所有子空间的格，

335

$$\mu(U,W)=\begin{cases}(-1)^k q^{\binom{k}{2}} & \text{如果 } U\subseteq W \text{ 且 } \dim(W)-\dim(U)=k,\\ 0 & \text{如果 } U\nsubseteq W.\end{cases}$$

(iv)对一个 $n$-集合 $X$ 的所有划分的格 $\Pi_n$，

$$\mu(\mathcal{A},\mathcal{B})=(-1)^{|\mathcal{A}|-|\mathcal{B}|}\prod_{B\in\mathcal{B}}(n_B-1)!,$$

$\mathcal{A}$, $\mathcal{B}$ 是 $\Pi_n$ 的满足 $\mathcal{A}\leq\mathcal{B}$ 的元素，这里 $n_B$ 表示包含在$\mathcal{B}$的一个区组 $B$ 中的$\mathcal{A}$的区组数.

(v)对一个凸多面体的面的格，

$$\mu(A,B)=\begin{cases}(-1)^{\dim(B)-\dim(A)} & \text{如果 } A\subseteq B,\\ 0 & \text{否则}.\end{cases}$$

现在我们叙述默比乌斯反演原理. 设 $P$ 是一个有限偏序集且 $\mu$ 是其默比乌斯函数. 设 $f$, $g$, $h: P\to\mathbb{R}$ (或映入到任意一个加法群)是使得对所有 $x\in P$ 关系

$$g(x)=\sum_{a:a\leqslant x}f(a)\quad 和\quad h(x)=\sum_{b:b\geqslant x}f(b)$$

成立的函数. 那么, 对所有 $x\in P$, 有

$$f(x)=\sum_{a:a\leqslant x}\mu(a,x)g(a) \tag{25.4}$$

和

$$f(x)=\sum_{b:b\geqslant x}\mu(x,b)h(b). \tag{25.5}$$

这些等式容易由直接代入验证. 例如, (25.4)的右端是

$$\sum_{a:a\leqslant x}\mu(a,x)\Big(\sum_{b:b\leqslant a}f(b)\Big)=\sum_{b:b\leqslant x}f(b)\left[\sum_{a:b\leqslant a\leqslant x}\mu(a,x)\right].$$

但由(25.3), 上式右端括号内的和除 $b=x$ 之外为零, 因此只有 $f(x)$ 留下. 或者, 由矩阵记号(我们把 $f$, $g$, $h$ 当作行或列向量——哪一个方便就采用哪一个——其坐标由 $P$ 标号), 被假定的 $g$ 和 $h$ 的关系, 等价于 $g=\zeta f$, 因此 $f=\mu g$; $h=f\zeta$, 因此 $f=h\mu$. [336]

当默比乌斯反演原理应用于一个集合 $X$ 的子集的格时, 我们回到容斥原理. 设 $(A_i: i\in I)$是一个有限集合 $X$ 的子集的有限族, 对 $J\subseteq I$, 设 $f(J)$等于 $X$ 的元素数, 这些元素恰好属于集合 $A_j(j\in J)$而不属于其他集合. (想一下在集合的文氏图中一个区域的规模.)设 $g(J)$等于在 $\bigcap_{j\in J}A_j$ 中元素的数目, 则 $g(J)=\sum_{K:J\subseteq K}f(K)$,因此默比乌斯反演给出

$$f(J)=\sum_{K:J\subseteq K}(-1)^{|K\setminus J|}g(K).$$

在 $J=\varnothing$的情形, 上式可写作

$$\Big|X-\bigcup_{i\in I}A_i\Big|=\sum_{K\subseteq I}(-1)^{|K|}\Big|\bigcap_{j\in K}A_j\Big|,$$

这是陈述容斥原理的隐秘方式.

当默比乌斯反演原理应用于一个整数 $n$ 的(正)因子的格时, 我们回到经典的数论默比乌斯反演. 如果 $f$ 和 $g$ 满足

$$g(m)=\sum_{k\mid m}f(k)\quad 对所有的 m 整除 n,$$

默比乌斯反演给出

$$f(m)=\sum_{k\mid m}\mu(k,m)g(k)\quad 对所有的 m 整除 n.$$

根据定理 25.1(ii), 这等价于定理 10.4.

我们给出例 10.2 的一个 $q$-类似, 那里我们利用容斥原理发现, 从一个 $n$-集到一个 $m$-集的满射的数目的表达式为 $\sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}k^n$. [337]

**定理 25.2** $\mathbb{F}_q$ 上从一个 $n$ 维向量空间到一个 $m$ 维向量空间 $V$ 的满射的线性变换数目是

$$\sum_{k=0}^{m}(-1)^{m-k}\begin{bmatrix}m\\k\end{bmatrix}_q q^{nk+\binom{m-k}{2}}.$$

**证明** 对一个子空间 $U\subseteq V$，设 $f(U)$ 表示其象为 $U$ 的线性变换的数目. 设 $g(U)$ 表示其象包含在 $U$ 中的线性变换的数目. 显然

$$g(U)=\sum_{W:W\subseteq U}f(W),$$

且如果 $\dim(U)=r$，则 $g(U)$ 等于 $q^{nr}$. 由 $V$ 的子空间的格上的默比乌斯反演，

$$f(U)=\sum_{W:W\subseteq U}\mu(W,U)q^{n\dim(W)}.$$

取 $U=V$ 并用定理 25.1(iii)得出定理叙述的结果. ■

**推论** 域 $\mathbb{F}_q$ 上秩为 $r$ 的 $n\times m$ 矩阵的数目是

$$\begin{bmatrix}m\\r\end{bmatrix}_q\sum_{k=0}^{r}(-1)^{r-k}\begin{bmatrix}r\\k\end{bmatrix}_q q^{nk+\binom{r-k}{2}}.$$

我们注意到，单射的线性变换的数目有相对简单的形式. 如果固定 $n$ 维向量空间的一组基并考虑到 $m$ 维向量空间的单射，第 $i$ 个基向量的象一定要从不在前面的基向量的象的生成中选取一个，即从 $(q^m-q^{i-1})$ 个向量中选一个. 总之，有 $(q^m-1)(q^m-q)\cdots(q^m-q^{n-1})$ 个单射的线性变换. 因为定理 25.2 在 $m=n$ 时也给出这个数目的表达式，所以我们已经证明了一个恒等式.

338

**问题 25A** (i)应用默比乌斯反演导出一个 $k$-子空间的数目的表达式，这些子空间与 $\mathbb{F}_q$ 上 $n$ 维向量空间的一个给定的 $r$-子空间平凡相交. 这给出等式(10.5)的 $q$-类似. (ii)对特殊情形 $r+k=n$，从另一个观点，通过考虑 $\mathbb{F}_q$ 上形如 $(I\ M)$ 的 $r\times n$ 矩阵证明恰有 $q^{rk}$ 个这样的子空间，这里 $I$ 是 $r$ 阶的单位阵.

**问题 25B** 利用默比乌斯反演导出 $\mathbb{F}_q$ 上一个 $n$ 维向量空间到自身的非奇异线性映射的数目，映射除 $\mathbf{0}$ 之外不保持其他向量不动，即它们不以 1 作为一个特征值. (这些映射是加法群的正交态射，见定理 22.9 之后的“注记”.)

* * *

定理 25.1 中提到的偏序集都是格. 下面这个有用的定理由 L. Weisner(1935)发现.

**定理 25.3** 设 $\mu$ 是一个有限格 $L$ 的默比乌斯函数且设 $a\in L$ 满足 $a>0_L$，则

$$\sum_{x:x\vee a=1_L}\mu(0_L,x)=0.$$

**证明** 固定 $a$ 并考虑

$$S:=\sum_{x,y\in L}\mu(0,x)\zeta(x,y)\zeta(a,y)\mu(y,1)=\sum_{x\in L}\sum_{\substack{y\geq x\\ y\geq a}}\mu(0,x)\mu(y,1).$$

一方面，

$$S=\sum_{x}\mu(0,x)\sum_{\substack{y\geq x\\ y\geq a}}\mu(y,1);$$

但 $y\geq a$ 且 $y\geq x$ 当且仅当 $y\geq x\vee a$，且内和是

339

$$\sum_{y\geq x\vee a}\mu(y,1)=\begin{cases}1 & 若\ x\vee a=1,\\ 0 & 若\ x\vee a<1.\end{cases}$$

因此 $S$ 是该定理陈述中的和. 另一方面，

$$S = \sum_{y \geq a} \mu(y,1) \sum_{0 \leq x \leq y} \mu(0,x),$$

因为 $y>0$，内和总是 0. ■

**推论** 对几何格 $L$ 中 $x \leqslant y$ 的两个元素 $x$，$y$，$\mu(x, y)$的符号为$(-1)^{\mathrm{rank}(y)-\mathrm{rank}(x)}$，特别地，$\mu(x, y)$从不为 0.

**证明** 对 $L$ 的秩我们用归纳法证明 $\mu(0_L, 1_L)$的符号为$(-1)^{\mathrm{rank}(L)}$. 取一个点 $p \in L$. 由半模性，$a \vee p = 1_L$ 当且仅当 $a = 1_L$ 或 $a$ 是不在 $p$ 上的一个上点；因此 Weisner 定理(即定理 25.3)给出

$$\mu(0_L, 1_L) = -\sum_{h: h \lessdot 1_L, h \ngeq p} \mu(0_L, h). \tag{25.6}$$

因为由归纳假设，等式右端的所有项的符号为$(-1)^{\mathrm{rank}(L)-1}$，证明完成. ■

由第 23 章引入的格 $L(G)$上的默比乌斯反演，可得到一个图 $G$ 用 $x$ 种颜色正常染色的数目$\mathcal{X}_G(x)$，尽管这未必是一个很实用的方法. 回忆 $L(G)$的元素是 $G$ 的顶点集的划分$\mathcal{A}$，其区组导出的 $G$ 的子图都是连通的. 对 $L(G)$中的$\mathcal{A}$，设 $g(\mathcal{A})$表示从 $G$ 的顶点集到 $x$ 种颜色的集合的映射数，使得$\mathcal{A}$的每个区组得到相同的颜色(即染色). 显然 $g(\mathcal{A}) = x^{|\mathcal{A}|}$. 设$f(\mathcal{A})$表示在$\mathcal{A}$的每个区组上是常数，但使得连结不同区组的边的端点得到不同染色的映射数. 给定由 $g(\mathcal{A})$"计数的"一个染色，不难想到有一个唯一的粗略划分$\mathcal{B}$，使得该染色由$f(\mathcal{B})$"计数"(必须联合$\mathcal{A}$的同色的两个区组，如果有一边连结它们). 因此 $g(\mathcal{A}) = \sum_{\mathcal{B} \geq \mathcal{A}} f(\mathcal{B})$，默比乌斯反演给出

$$f(\mathcal{A}) = \sum_{\mathcal{B} \geq \mathcal{A}} \mu(\mathcal{A}, \mathcal{B}) g(\mathcal{B}).$$

[340]

正常染色的数目是 $f$ 在 $0_{L(G)}$(分成单元素集的划分)上求值，即

$$\mathcal{X}_G(x) = \sum_{\mathcal{B}} \mu(0_{L(G)}, \mathcal{B}) x^{|\mathcal{B}|} = \sum_{k=1}^{n} \Big( \sum_{|\mathcal{B}|=k} \mu(0_{L(G)}, \mathcal{B}) \Big) x^k.$$

多项式$\mathcal{X}_G(x)$称为该图的色多项式. 上面的推论直接导出下面的陈述.

**定理 25.4** $n$ 个顶点的一个图$G$ 用 $x$ 种颜色正常染色的数目由次数为$n$ 的一个首 1 多项式$\mathcal{X}_G(x)$确定，其系数的符号正、负交错.

**问题 25C** 设 $G$ 是一个有 $n$ 个顶点和 $m$ 条边的简单图. 证明在$\mathcal{X}_G(x)$中 $x^{n-1}$的系数是$-m$，$x^{n-2}$的系数是 $m(m-1)/2$ 减去 $G$ 中的三角形的数目.

T. Dowling and R. M. Wilson(1975)证明了下面的定理及其推论，后者是关于线性空间的定理 19.1 中不等式的推广.

**定理 25.5** 如果 $L$ 是一个有限格，使得对所有的 $x \in L$ 有$\mu(x, 1_L) \neq 0$，则存在 $L$ 的元素的一个置换 $\pi$，使得对所有的 $x \in L$，$x \vee \pi(x) = 1_L$.

**证明** 在开始证明之前，我们说不满足假设的格有多于两个元素的链. 当然，不存在有上述性质的置换 $\pi$. 另一方面，一个 $n$-集合的所有子集的格有一个唯一的置换具有上面的性质，即把每个子集映到这个子集的补的置换.

这里所有矩阵的行和列由 $L$ 标号. 设

341

$$\eta(x,y):=\begin{cases}1 & \text{如果 } x\vee y=1_L,\\ 0 & \text{否则.}\end{cases}$$

设 $\delta_1$ 为满足 $\delta_1(x, x):=\mu(x, 1_L)$ 的对角矩阵. 因为

$$\begin{aligned}\zeta\delta_1\zeta^{\top}(x,y)&=\sum_{a,b}\zeta(x,a)\delta_1(a,b)\zeta(y,b)\\&=\sum_{a:a\geqslant x\text{且}a\geqslant y}\delta_1(a,a)\\&=\sum_{a:a\geqslant x\vee y}\mu(a,1_L)\end{aligned}$$

由(25.1), 最后的和当 $x\vee y=1_L$ 时等于 1, 否则等于 0, 故 $\zeta\delta_1\zeta^{\top}=\eta$.

在 $\mu(x, 1_L)\neq 0$ 的假设下, 矩阵 $\delta_1$ 是非奇异的. 因为 $\zeta$ 也是非奇异的, 我们得出 $\eta$ 非奇异的结论. 因此在这个行列式的展开中某一项不为零, 这蕴涵定理的结论. ■

**推论** *在一个秩为 $n$ 的有限几何格中, 秩 $\geqslant n-k$ 的元素数至少等于秩 $\leqslant k$ 的元素数, 这里 $0\leqslant k\leqslant n$.*

**证明** 考虑如定理 25.5 中那样的置换 $\pi$(它适用是因为定理 25.3 的推论). 半模律

$$\operatorname{rank}(x)+\operatorname{rank}(\pi(x))\geqslant\operatorname{rank}(x\vee\pi(x))+\operatorname{rank}(x\wedge\pi(x))\geqslant n$$

蕴涵一个秩 $\leqslant k$ 的元素的象是一个秩 $\geqslant n-k$ 的元素. ■

我们给出 T. Dowling(1977)关于补置换定理的一个类似的矩阵证明.

**定理 25.6** *如果 $L$ 是一个对所有 $x\in L$ 使得 $\mu(x, 1_L)\neq 0$ 且 $\mu(0_L, x)\neq 0$ 的有限格, 则存在 $L$ 的元素的一个置换 $\pi$ 使得对所有的 $x\in L$,*

$$x\vee\pi(x)=1_L\quad\text{和}\quad x\wedge\pi(x)=0_L.$$

**证明** 设 $\delta_1$ 如同前一个定理的证明中一样, 设 $\delta_0$ 是满足 $\delta_0(x, x):=\mu(0_L, x)$ 的对角矩阵. 现在假设 $\kappa:=\zeta\delta_1\zeta^{\top}\delta_0\zeta$, 这蕴涵 $\kappa$ 是非奇异的. 我们断言 $\kappa(x, y)=0$, 除 $x$ 和 $y$ 是互补的外. 那么对应于 $\kappa$ 的行列式展开中一个非零项的任何置换是补置换.

342

为了建立我们的断言, 首先注意到 $\kappa=\eta\delta_0\zeta$, 因此

$$\kappa(x,y)=\sum_{z:z\vee x=1_L,z\leqslant y}\mu(0_L,z).$$

如果这个和不等于零, 则存在某个 $z$, 使得 $z\vee x=1_L$ 且 $z\leqslant y$, 这蕴涵 $y\vee x=1_L$. 由对偶性, $\eta'=\zeta^{\top}\delta_0\zeta$, 其中

$$\eta'(x,y):=\begin{cases}1 & \text{如果 } x\wedge y=0_L,\\ 0 & \text{否则.}\end{cases}$$

注意 $\kappa=\zeta\delta_1\eta'$, 而且类似地 $\kappa(x, y)\neq 0$ 蕴涵 $x\wedge y=0_L$. ■

最后, 给出在本章开始时我们允诺的证明.

**定理 25.1 的证明** (i)因为区间$[A, B]$与 $B\setminus A$ 的子集的格同构, 只要证得 $\mu(\varnothing, C)=(-1)^{|C|}$ 即可. 我们利用等式(25.6)并对 $|C|$ 用归纳法. 设 $p$ 是 $C$ 中的一点. 只存在一个不在 $p$ 上的上点, 即$\{p\}$的补. 因此(25.6)蕴涵

$$\mu(\varnothing,C)=-\mu(\varnothing,C\setminus\{p\})=-(-1)^{(|C|-1)}=(-1)^{|C|}.$$

(ii)计算$\mu(1, m)$就够了，而且我们对$m$用归纳法．设$p$是$m$的一个素因子．Weisner 定理断定

$$\mu(1,m) = -\sum_{\operatorname{lcm}(a,p)=m, a<m} \mu(0,a).$$

如果$p^2$整除$m$，则上式右端的和是零，因此$\mu(1, m)=0$．如果$p^2$不整除$m$，则存在一项，即$a=m/p$的情形．

343

(iii)对$k$维的空间$V$证明$\mu(0, V)=(-1)^k q^{\binom{k}{2}}$就够了．我们对$k$用归纳法．设$p$为$V$的一个 1 维子空间．由 Weisner 定理，

$$\mu(0,V) = -\sum_{U:U\vee P=V, U\neq V} \mu(0,U).$$

由归纳假设，在上面的和中，每一项$\mu(0, U)$等于$(-1)^{k-1}q^{\binom{k-1}{2}}$．除$V$之外使得$U\vee P=V$的子空间仅仅是那些不包含$P$的$k-1$维子空间$U$，它们的数目是

$$\begin{bmatrix} k \\ 1 \end{bmatrix}_q - \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q = q^{k-1}.$$

这就完成了(iii)的证明．

(iv)考虑$\mathcal{A}\leq\mathcal{B}$的两个划分$\mathcal{A}$和$\mathcal{B}$．比如说$\mathcal{B}$有$k$个区组，当标号时，分别是$\mathcal{A}$的$n_1$，$n_2$，…，$n_k$个区组的并．则区间$[\mathcal{A}, \mathcal{B}]$同构于划分格的直积

$$\Pi_{n_1} \times \Pi_{n_2} \times \cdots \times \Pi_{n_k},$$

原因是对每个$i=1, 2, \cdots, k$，满足$\mathcal{A}\leq\mathcal{C}\leq\mathcal{B}$的一个划分$\mathcal{C}$由$\mathcal{A}$的$n_i$个区组的一个划分指定，这$n_i$个区组落在$\mathcal{B}$的第$i$个区组中．

我们现在考虑这一事实，即$P$和$Q$为两个偏序集，$\mu_P$和$\mu_Q$分别是它们的默比乌斯函数，直积$P\times Q$的默比乌斯函数$\mu_{P\times Q}$是$\mu_P$和$\mu_Q$的(克罗内克或张量)积，即

$$\mu_{P\times Q}((a_1,b_1),(a_2,b_2)) = \mu_P(a_1,a_2)\mu_Q(b_1,b_2).$$

(对此我们留给读者思考，只要检验上面定义的$\mu_{P\times Q}$产生$\zeta_{P\times Q}$的一个逆．)因此对$i=1, 2\cdots, k$，$\mu(\mathcal{A}, \mathcal{B})$是$\mu(0_{\Pi_{n_i}}, 1_{\Pi_{n_i}})$的积．

344

现在我们由对$n$进行归纳证明$\mu(0_{\Pi_n}, 1_{\Pi_n})=(-1)^{n-1}(n-1)!$．设$\mathcal{P}$为$\Pi_n$的一个点，即一个$n$-集合划分成一个 2-集合$\{x, y\}$和$n-2$个单元素集的一个划分．使得$\mathcal{P}\vee\mathcal{A}=1_{\Pi_n}$的划分$\mathcal{A}$是带两个区组的$2^{n-2}$个划分，这两个区组分离$x$和$y$的划分，有$\binom{n-2}{i}$个，这里包含$x$的区组的规模为$i+1$，包含$y$的区组的规模为$n-1-i$．由(25.6)和归纳假设，

$$\begin{aligned} \mu(0_{\Pi_n}, 1_{\Pi_n}) &= -\sum_{i=0}^{n-2} \binom{n-2}{i} (-1)^i (i)! (-1)^{n-2-i} (n-2-i)! \\ &= (-1)^{n-1}(n-1)!. \end{aligned}$$

■

**问题 25D** Weisner 定理的对偶(应用定理 25.3 于对偶格导出)断定

$$\sum_{x:x\wedge a=0_L} \mu(x,1_L) = 0 \quad 对满足 a < 1_L 的所有 a \in L.$$

取$a$为一个划分，它的一个区组的规模为$n-1$且另一个区组的规模为 1(在划分格中)，用上面的对偶给$\mu(0_{\Pi_n}, 1_{\Pi_n})=(-1)^{n-1}(n-1)!$一个稍微不同的证明．

我们用划分格上的默比乌斯反演，得出 $n$ 个顶点上连通的标号简单图的数目．设 $X$ 是一个 $n$-集合．对点集为 $X$ 的每个图 $G$，对应 $X$ 的划分 $\mathcal{C}_G$，$\mathcal{C}_G$ 的区组是 $G$ 的连通分支的顶点集．我们用 $g(\mathcal{B})$ 表示满足 $V(G)=X$ 且 $\mathcal{C}_G=\mathcal{B}$ 的简单图 $G$ 的数目，用 $f(\mathcal{B})$ 表示满足 $V(G)=X$ 且 $\mathcal{C}_G$ 是 $\mathcal{B}$ 的一个细分的简单图 $G$ 的数目．显然，

$$f(\mathcal{B}) = \sum_{\mathcal{A}\le\mathcal{B}} g(\mathcal{A}).$$

我们对 $g(1_{\Pi_n})$ 感兴趣，这里 $1_{\Pi_n}$ 是有一个区组的划分．但容易计算的是 $f(\mathcal{B})$，通过在 $B$ 的每个区组上随意选择一个简单图，由 $f(\mathcal{B})$ 可以得到一个图的计数，因此如果 $\mathcal{B}$ 有规模为 $i$ 的 $k_i$ 个区组，则

345

$$f(\mathcal{B}) = 2^{k_2\binom{2}{2}}2^{k_3\binom{3}{2}}\cdots 2^{k_n\binom{n}{2}}.$$

由默比乌斯反演，

$$g(\mathcal{B}) = \sum_{\mathcal{A}\le\mathcal{B}} \mu(\mathcal{A},\mathcal{B}) f(\mathcal{A}).$$

指定 $\mathcal{B}=1_{\Pi_n}$，我们有

$$g(1_{\Pi_n}) = \sum_{\mathcal{A}} \mu(\mathcal{A},1_{\Pi_n}) f(\mathcal{A}). \tag{25.7}$$

回忆类型为 $(k_1,\ k_2,\ \cdots,\ k_n)$ 的 $X$ 的划分数是

$$\frac{n!}{(1!)^{k_1}k_1!(2!)^{k_2}k_2!\cdots(n!)^{k_n}k_n!};$$

参见(13.3)．应用定理 25.1(iv)，我们发现有 $n$ 个顶点的连通标号图的数目是

$$\sum(-1)^{k_1+k_2+\cdots+k_n-1}\frac{n!(k_1+\cdots+k_n-1)!}{(1!)^{k_1}k_1!\cdots(n!)^{k_n}k_n!}2^{k_2\binom{2}{2}+k_3\binom{3}{2}+\cdots+k_n\binom{n}{2}},$$

这里求和遍及整数 $n$ 的所有划分 $(k_1,\ k_2,\ \cdots,\ k_n)$，这就是所有满足 $1k_1+2k_2+\cdots+nk_n=n$ 的非负 $n$ 元组．

这不意味着这个结果是原始问题的一个特别好的答案．事实上，这是在一个大的对象集上求和，对象的数目对大的 $n$ 超过 $e^{\sqrt{n}}$．但这是默比乌斯反演的一个自然的例证，而且大大地简化了问题．对 $n=5$，我们有

| 5 的划分 | $\mathcal{A}$ 的数目 | $f(\mathcal{A})$ | $\mu(\mathcal{A},\ 1_{\Pi_5})$ |
|---|---|---|---|
| 5 | 1 | 1024 | 1 |
| 41 | 5 | 64 | −1 |
| 32 | 10 | 16 | −1 |
| 311 | 10 | 8 | 2 |
| 221 | 15 | 4 | 2 |
| 2111 | 10 | 2 | −6 |
| 11111 | 1 | 1 | 24 |

346

从这个表和(25.7)可以看到，在 5 个顶点的 1024 个标号的简单图中有 728 个是连通的．

* * *

我们给出默比乌斯反演对编码理论的一个应用．回忆在例 20.3 中给出的 MDS 码的定义．

设 $C$ 是这样一个码，即$\mathbb{F}_q$ 上一个满足 $d=n-k+1$ 的$[n, d, k]$码. 如果我们考虑 $d$ 个位置的一个集合，然后观察在其他位置上全为零的 $C$ 的子码，这个子码的维数$\geqslant k-(n-d)=1$. 因为这个子码有最小距离 $d$，由定理 20.2，它的维数一定恰好是 1. 由此得出，对 $n\geqslant d'>d$，指定 $d'$个位置的一个集合且要求码字在其他所有的位置为零，这定义一个维数为 $d'-d+1$ 的 $C$ 的子码. 在下面的证明中要用到这点. 我们将证明一个 MDS 码的重量计数器由其参数确定.

**定理 25.7** 设 $C$ 是一个$\mathbb{F}_q$ 上距离 $d=n-k+1$ 的$[n, k]$码. 则 $C$ 的重量计数器是 $1+\sum_{i=d}^{n}A_i z^i$，这里

$$A_i=\binom{n}{i}(q-1)\sum_{j=0}^{i-d}(-1)^j\binom{i-1}{j}q^{i-j-d},\quad i=d, d+1, \cdots, n.$$

**证明** 设 $R$ 是 $N:=\{0, 1, \cdots, n\}$的一个子集. 定义 $f(R)$为满足$\{i: c_i\neq 0\}=R$ 的码字$(c_0, c_1, \cdots, c_{n-1})$的数目. 对 $N$ 的一个子集 $S$，我们定义 $g(S):=\sum_{R\subseteq S}f(R)$. 如上面所说，我们有

$$g(S)=\begin{cases}1 & \text{如果 } |S|\leqslant d-1,\\ q^{|S|-d+1} & \text{如果 } n\geqslant |S|\geqslant d.\end{cases}$$

$f$ 的定义蕴涵 $A_i=\sum_{R\subseteq N, |R|=i}f(R)$. 现在我们应用定理 25.1(i)中的默比乌斯反演，发现

347

$$\begin{aligned}A_i&=\sum_{R\subseteq N, |R|=i}\ \sum_{S\subseteq R}\mu(S, R)g(S)\\&=\binom{n}{i}\left\{\sum_{j=0}^{d-1}\binom{i}{j}(-1)^{i-j}+\sum_{j=d}^{i}\binom{i}{j}(-1)^{i-j}q^{j-d+1}\right\}\\&=\binom{n}{i}\sum_{j=d}^{i}\binom{i}{j}(-1)^{i-j}(q^{j-d+1}-1).\end{aligned}$$

如果用 $i-j$ 代替 $j$ 并利用$\binom{i}{j}=\binom{i-1}{j-1}+\binom{i-1}{j}$，就得到定理的结论. ■

定理 25.7 蕴涵对 MDS 码的字母表的规模有相当严格的限制.

**推论** 如果$\mathbb{F}_q$ 上存在长度为 $n$ 且维数为 $k$ 的一个 MDS 码，则

$$\begin{cases}\text{(i)} & q\geqslant n-k+1 \text{ 或 } k\leqslant 1,\\ \text{(ii)} & q\geqslant k+1 \text{ 或 } d=n-k+1\leqslant 2.\end{cases}$$

**证明** (i)设 $d=n-k+1$. 由定理 25.7 可以发现，对 $d<n$，

$$0\leqslant A_{d+1}=\binom{n}{d+1}(q-1)(q-d).$$

(ii)设 $G:=(I_k\quad P)$是 $C$ 的生成矩阵. 因为 $C$ 有最小重量 $d$，奇偶校验矩阵 $H:=(-P^{\top}\quad I_{n-k})$的 $d-1=n-k$ 列的每个集合是线性无关的. 于是 $H$ 的每个子方阵是非奇异的. 因此，$C^{\perp}$ 中没有一个码字有 $n-k$ 个零，即 $C^{\perp}$ 也是 MDS. 应用(i)的结果于 $C^{\perp}$. ■

**问题 25E** 设 $P$ 为一个偏序集. 回忆如果 $x<y$，那么序列 $x=x_0<x_1<\cdots<x_k=y$ 称为从

$x$ 到 $y$ 长度为 $k$ 的一个链．设 $c_k(x, y)$ 表示这种链的数目(因此 $c_1(x, y)=1$)．证明

348

$$\mu(x,y) = \sum_{k\geq 1}(-1)^k c_k(x,y).$$

**问题 25F** 我们考虑向量空间 $V := \mathbb{F}_q^n$ 的子空间的格．设 $S$ 为 $\mathbb{F}_q$ 上的另一个向量空间．定义一个子空间 $U$：

$f(U) :=$ 以 $U$ 为核的从 $V$ 到 $S$ 的线性映射的数目，

$g(U) :=$ 以包含 $U$ 的集合为核的从 $V$ 到 $U$ 的线性映射的数目．

(i)确定 $g(U)$，然后把默比乌斯反演用于

$$g(U) = \sum_{W:W\supseteq U} f(W).$$

(ii)证明

$$f(\{\mathbf{0}\}) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (-1)^k q^{\binom{k}{2}} \mid S \mid^{n-k}.$$

(iii)证明多项式的恒等式

$$\prod_{k=0}^{n-1}(x-q^k) = \sum_{k=0}^{n}(-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{k}{2}} x^{n-k}.$$

## 评注

用 $L(G)$ 的默比乌斯函数表示的图的色多项式归功于 G.-C. Rota(1964).

定理 25.1(v)本质上是多面体的欧拉公式：

$$f_0 - f_1 + f_2 - f_3 + \cdots + (-1)^n f_n = 0,$$

这里 $f_i$ 是秩为 $i$ 或维数为 $i-1$ 的面的数目($f_0 = f_n = 1$)．见 B. Grünbaum(1967)．也见 R. Stanley(1986)，这里偏序集称为欧拉偏序集，具有性质：只要 $x$ 和 $y$ 的秩相差 $d$，就有 $\mu(x, y)=(-1)^d$.

## 参考文献


T. Dowling (1977), A note on complementing permutations, *J. Combinatorial Theory* (B) **23**, 223–226.

349

T. Dowling and R. M. Wilson (1975), Whitney number inequalities for geometric lattices, *Proc. Amer. Math. Soc.* **47**, 504–512.

B. Grünbaum (1967), *Convex Polytopes*, J. Wiley (Interscience).

G.-C. Rota (1964), On the foundations of combinatorial theory I. Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie* **2**, 340–368.

R. P. Stanley (1986), *Enumerative Combinatorics*, Vol. 1, Wadsworth.

L. Weisner (1935), Abstract theory of inversion of finite series, *Trans. Amer. Math. Soc.* **38**, 474–484.

350

# 第 26 章　组合设计和射影几何

有限域上的几何是组合设计以及相关组合构形的丰富源泉. 我们以两个主题(弧与子平面)开始，只限于在射影平面中叙述它们，然后讨论在一般射影空间中的二次曲面及其他构形.

在射影平面中，一个$(m, k)$-弧是$m$个点的一个集合，其中没有$k+1$个点共线. 在问题 19I 中我们关心$(m, 2)$-弧.

设$A$为$n$阶射影平面上的一个$(m, k)$-弧，再设$x$为$A$中的一个点. $x$上的$n+1$条线中的每一条至多包含$A$中除$x$之外的$k-1$个点，因此

$$m \leqslant 1 + (n+1)(k-1).$$

当上式中等号成立时，$(m, k)$-弧$A$称为*完全的*. 完全的$(m, k)$-弧中的任意一条线显然包含该弧的$k$个点，这就是，对任意一条线$L$，

$$|L \cap A| = 0 \text{ 或 } k.$$

显然，线与一条完全的$(m, k)$-弧的交(非空)提供了施泰纳系$S(2, k, m)$的区组.

单独一个点是完全的$(1, 1)$-弧. $n$阶射影平面上$n^2$个不在一条固定的直线上的点之集合是一个完全的$(n^2, n)$-弧，它对应的施泰纳系是一个$n$阶的仿射平面. 问题 19I 中的超卵形是完全的$(q+2, 2)$-弧. 它们对应的设计是平凡的. 但是有"对偶"弧，它们对应的施泰纳系是有趣的——见问题 26A.



下面的定理属于 R. H. F. Denniston(1969)，这个定理的部分(2)给出在偶数阶的德萨格平面上完全的$(m, k)$-弧的构造. 在奇数阶$n(1<k<n)$的射影平面上，现在还没有完全的$(m, k)$-弧的例子.

**定理 26.1**　*(1)如果在一个$n$阶的射影平面上存在一个完全的$(m, k)$-弧，则$k$整除$n$.*

*(2)如果$q$是 2 的幂且$k$整除$q$，则在$PG_2(q)$上存在一个完全的$(m, k)$-弧.*

**证明**　设$x$是不在一个完全的$(m, k)$-弧$A$上的点，$A$在一个$n$阶的射影平面上. $x$上的线划分其余的点，但$x$上的每条线恰包含$A$的 0 或$k$个点. 于是$k$一定整除$m=1+(n+1)(k-1)$. 由此$k$整除$n$.

现在设$q$是 2 的幂且$k$是$q$的一个因子，设$f(x, y)=\alpha x^2+\beta xy+\gamma y^2$是$\mathbb{F}_q$上的不可约二次式，又设$H$为$\mathbb{F}_q$的加法群的$k$阶子群. 在仿射平面$AG(2, q)$上，设

$$A := \{(x,y) : f(x,y) \in H\}.$$

我们断言任意(仿射)直线交$A$于 0 或$k$个点. 当这一仿射平面嵌入在$PG_2(q)$中时，$A$将是一个完全的$(m, k)$-弧.

考虑$b$和$m$都不是零的一条直线$L=\{(x, y) : y=mx+b\}$. (形如$\{(x, y) : y=mx\}$和$\{(x, y) : x=c\}$的直线留给读者考虑.)

交$L \cap A$是点$(x, mx+b)$的集合，这里

$$\alpha x^2 + \beta x(mx+b) + \gamma(mx+b)^2 \in H, \quad \text{或}$$

$$F(x)\in H,\quad 其中\quad F(x):=(\alpha+\beta m+\gamma m^2)x^2+\beta bx+\gamma b^2.$$

我们采用的是特征为 2 的域，因此

$$x\mapsto(\alpha+\beta m+\gamma m^2)x^2+\beta bx$$

352 是一个线性映射；它有阶为 2 的核，因为 $f(x,y)$的不可约性保证 $\beta$ 和 $x^2$ 的系数都不为零. 于是，这个映射的象 $K_F$ 是$\mathbb{F}_q$ 的加法群的 $q/2$ 阶子群. $F$ 的象是 $K_F$ 的一个陪集，但因为 $F(x)$总不为零(又由 $f(x,y)$的不可约性)，$F$ 的象是补$\mathbb{F}_q\setminus K_F$. 总之，

$$|\{x:F(x)\}=a\}|=\begin{cases}2 & 如果\ x\notin K_F,\\ 0 & 如果\ x\in K_F.\end{cases}$$

因此 $|L\cap A|=2|H\cap(\mathbb{F}_q\setminus K_F)|$. 子群 $H$ 或者包含在 $K_F$ 中，在这一情形 $L\cap A=\varnothing$；或者交 $K_F$ 于一个 $k/2$ 阶子群，在这一情形 $|L\cap A|=k$. ■

作为这个定理的一个推论($n=2^{m+1}$，$k=2^m$)，我们得到施泰纳系

$$S(2,2^m,2^{2m+1}-2^m).$$

当 $v$ 接近 $k^2$ 时，施泰纳系 $S(2,k,v)$在许多方面是令人感兴趣的，如对仿射平面和射影平面的情形(费希尔不等式，即定理 19.6，证明 $v\geqslant k^2-k+1$). 这些例子有 $v<2k^2$，但仍给人以深刻的印象.

**问题 26A** 设 $A$ 是 $n$ 阶射影平面 $P$ 中的一个完全的$(m,k)$-弧，其中 $1\leqslant k\leqslant n$. 设 $A^*$ 为不与 $A$ 相交的线的集合. 证明 $A^*$ 是 $P$ 的对偶平面 $P^*$ 中的一个完全的$(m^*,[n/k])$-弧，并用 $m$，$k$ 和 $n$ 计算 $m^*$.

**问题 26B** 施泰纳系 $S(2,k,m)$的一个平行类是 $m/k$ 个区组的一个集合$\mathcal{A}$，使得每个点恰与$\mathcal{A}$中的一个区组关联. 当 $S(2,k,m)$的区组能划分成平行类时，$S(2,k,m)$是可分解的(参见问题 19K).

设 $A$ 是 $n$ 阶射影平面 $P$ 中的一个完全的$(m,k)$-弧. 施泰纳系 $S(2,k,m)$的区组是线与 $A$ 的非平凡的交，解释为何 $S(2,k,m)$是可分解的.

射影平面 $\boldsymbol{P}$ 的子平面 $\boldsymbol{S}$ 是 $\boldsymbol{P}$ 的一个子结构，从它自身的性质来看它是一个射影平面. 回忆关联结构$(\mathcal{P},\mathcal{B},\boldsymbol{I})$的一个子结构是关联结构$(\mathcal{P}_0,\mathcal{B}_0,\boldsymbol{I}_0)$，这里$\mathcal{P}_0\subseteq\mathcal{P}$，$\mathcal{B}_0\subseteq\mathcal{B}$且 $\boldsymbol{I}_0=$
353 $\boldsymbol{I}\cap(\mathcal{P}_0\times\mathcal{B}_0)$. 注意，给定射影平面 $\boldsymbol{P}$ 的一个自同构(或直射变换)$\alpha$，子结构 $\boldsymbol{S}$ 由被$\alpha$ 固定的$\boldsymbol{P}$ 的点和由 $\alpha$ 固定的 $\boldsymbol{P}$ 的线构成，子结构 $\boldsymbol{S}$ 具有以下性质：$\boldsymbol{S}$ 的两个点与 $\boldsymbol{S}$ 的唯一一条线关联，且 $\boldsymbol{S}$ 的两条线与 $\boldsymbol{S}$ 的唯一一个点关联. 如果 $\boldsymbol{S}$ 包含四个点，没有三点共线，则 $\boldsymbol{S}$ 是一个子平面，但它也可能是一个拟束或者有一条线或者没有线.

**例 26.1** 设 $V:=\mathbb{F}_{q^n}^3$. $PG_2(q^n)$的点和线都是 $V$ 的 1 维和 2 维$\mathbb{F}_{q^n}$-子空间. 定义 $PG_2(q^n)$的一个子结构 $\boldsymbol{S}$，$\boldsymbol{S}$ 的点和线是 $V$ 的这样一些 1 维和 2 维的$\mathbb{F}_q$的子空间，使子空间的基由元素在子域$\mathbb{F}_q$里的向量构成. 则 $\boldsymbol{S}$ 是一个子平面. $\boldsymbol{S}$ 中的一条线与 $PG_2(q^n)$中的 $q^n+1$ 个点关联，但其中仅有 $q+1$ 个 $\boldsymbol{S}$ 中的点.

**定理 26.2** 如果一个 $n$ 阶射影平面$\boldsymbol{P}$ 包含 $m$ 阶的一个子平面$\boldsymbol{S}$，其中 $m<n$，则或者
(i)$n=m^2$，或者
(ii)$n\geqslant m^2+m$.

**证明** 设 $\boldsymbol{L}$ 为子平面 $\boldsymbol{S}$ 中的一条线，$L$ 中的一个点 $x$ 在 $\boldsymbol{P}$ 中但不在 $\boldsymbol{S}$ 中. $x$ 上的其他 $n$ 条线可以包含 $\boldsymbol{S}$ 中至多一个点(因为在 $\boldsymbol{P}$ 中至少包含 $\boldsymbol{S}$ 中两个点的一条线 $M$ 必然属于子平面 $\boldsymbol{S}$，因此 $M$ 和 $L$ 的公共点 $x$ 也属于该子平面). 线 $L$ 包含 $\boldsymbol{S}$ 中的 $m+1$ 个点，它共有 $m^2+m+1$ 个点，每一个点在某一条过 $x$ 的线上，因此 $m^2\leqslant n$.

相等性蕴涵 $\boldsymbol{P}$ 的每条线与 $\boldsymbol{S}$ 相交(显然交于 1 或 $m+1$ 个点)，因为如果线 $N$ 不与 $\boldsymbol{S}$ 相交，$x$ 取作 $L$ 和 $N$ 的交点，则 $\boldsymbol{S}$ 的 $m^2$ 个点中不在 $L$ 上的点属于 $n-1$ 条线中的一条.

现在假设 $m^2<n$，所以存在一条线 $N$ 不与 $\boldsymbol{S}$ 的点关联. $\boldsymbol{S}$ 的 $m^2+m+1$ 条线中的每一条包含 $N$ 的一个点且两条这样的线不能包含同一点，故 $m^2+m+1\leqslant n+1$. ■

**问题 26C** 证明：如果 $PG_2(\mathbb{F})$ 包含费诺构形 $PG_2(2)$，则$\mathbb{F}$ 有特征 2. 提示：不失一般性，费诺构形的四个点是$<1, 0, 0>$，$<0, 1, 0>$，$<0, 0, 1>$和$<1, 1, 1>$. 计算其他三个点的齐次坐标(它们一定位于一条线上). [354]

**问题 26D** 在射影平面中，区组化集是一个点集 $S$，它不包含线但使得每一条线与 $S$ 交于至少一个点. 证明在 $n$ 阶射影平面中，一个区组化集至少包含 $n+\sqrt{n}+1$ 个点，且等号成立当且仅当 $S$ 是白尔子平面的点集.

我们用下面关于一类仿射区组化集的定理证明来描述“多项式方法”，该定理属于 Brouwer and Schrijver(1978).

**定理 26.3** 如果 $V$ 是 $AG(k, q)$的一个子集，它与所有的超平面相交，则

$$|V|\geqslant k(q-1)+1.$$

**证明** 设 $A$ 为区组化集. 不失一般性，设 $\mathbf{0}\in A$. 设 $B:=A\setminus\{\mathbf{0}\}$. 则 $B$ 与所有不含 $\mathbf{0}$ 的超平面相交. 这些超平面由方程 $w_1x_1+\cdots+w_kx_k=1$ 定义，这里 $\boldsymbol{w}$ 取遍所有非零向量. 因此

$$F(x_1,x_2,\cdots,x_k):=\prod_{b\in B}(b_1x_1+b_2x_2+\cdots+b_kx_k-1)$$

在该空间中除 $\mathbf{0}$ 之外恒等于 0.

由归纳法容易证明，在该空间上恒等于 0 的多项式一定在由多项式 $x_i^q-x_i(i=1, \cdots, k)$ 生成的理想中. 把 $F(x)$写作

$$F(x_1,\cdots,x_k)=\sum_{i=1}^{k}F_i(x_1,\cdots,x_k)(x_i^q-x_i)+G(x_1,\cdots,x_k),$$

这里在 $G$ 中 $x_i$ 的最高次数至多为 $q-1$. 对每个 $i$，多项式 $x_iF(x_1, \cdots, x_k)$恒等于 0，因此 $x_iG(x_1, \cdots, x_k)$也恒等于 0. 所以 $G$ 能被$\prod(x_i^{q-1}-1)$整除. 因为 $F(\mathbf{0})\neq 0$，$G(\mathbf{0})\neq 0$，所以 $G$ 的次数为 $k(q-1)$. 因此 $F$ 的次数(即 $|B|$)一定大于或等于 $k(q-1)$. ■

域$\mathbb{F}$ 上不定元为 $x_1, x_2, \cdots, x_n$ 的二次型是这些不定元的一个 2 次齐次多项式，即

$$f(\boldsymbol{x})=f(x_1,x_2,\cdots,x_n)=\sum_{i,j=1}^{n}c_{ij}x_ix_j, \tag{26.1}$$

[355]

这里系数 $c_{ij}$ 在$\mathbb{F}$ 中. 可能多个系数矩阵 $C=(c_{ij})$定义同一个二次型，因为只有对角元素及 $c_{ij}+c_{ji}$是重要的. 我们可以要求对 $i>j$，$c_{ij}=0$，则 $x_1, x_2, \cdots, x_n$ 的二次型与$\mathbb{F}$ 上的上三角 $n\times n$ 矩阵一一对应.

$PG_n(\mathbb{F})$中的二次曲面是一个射影点的集合

$$Q = Q(f) := \{\langle \boldsymbol{x} \rangle : f(\boldsymbol{x}) = 0\},$$

这里 $f$ 是 $n+1$ 个不定元的二次型. 为做出这个定义，我们一定要选择一组基并把向量与$\mathbb{F}$上的$(n+1)$元组等同.

两个二次型 $f$ 和 $g$ 是射影等价的，如果从 $f$ 通过一个"可逆线性替换"得到 $g$，或者用矩阵的记号，对$\mathbb{F}$上的某个 $n\times n$ 非奇异矩阵 $A$，$g(\boldsymbol{x})=f(\boldsymbol{x}A)$. 因此，如果 $f$ 如(26.1)中由一个矩阵 $C$ 给出，即 $f(\boldsymbol{x})=\boldsymbol{x}C\boldsymbol{x}^{\mathrm{T}}$，则 $g$ 由矩阵 $ACA^{\mathrm{T}}$ 给出. 例如，对任意的正整数 $n$，$nx_1^2+nx_2^2+nx_3^2+nx_4^2$ 在有理数域上与 $x_1^2+x_2^2+x_3^2+x_4^2$ 射影等价；见式(19.12).

我们说矩阵记号不会改变不定元的名称和数目，而这些改变是允许的. 例如，在二次型 $f$ 中用 $y_1+y_2$ 代替 $x_1$ 产生一个新的射影等价型，这里 $y_1$ 和 $y_2$ 是新的不定元.

一个二次型的秩是在任意的射影等价二次型中出现的不定元(系数不为零)的最小数目. 例如，$(x_1+\cdots+x_n)^2$ 的秩为 1. 射影等价二次型有相同的秩. 一个 $r$ 个不定元的二次型称为非退化的，如果它的秩为 $r$.

**例 26.2** 考虑两个不定元的二次型

$$f(x,y) = ax^2 + bxy + cy^2.$$

当且仅当 $a=b=c=0$ 时这个二次型的秩为 0. 它对应的二次曲面包含 $PG_1(\mathbb{F})$中的所有点(射影线). 如果不为零，它的秩为 1 当且仅当它是一个线性型 $dx+ey$ 的平方的标量倍，这是当且仅当判别式$b^2-4ac=0$ 的情形. 则它在 $PG_1(\mathbb{F})$中对应的二次曲面由单独一个点构成. 两个不定元的秩为 2 的二次型或者是不可约的，或者可以分解为两个线性型. 在第一种情形，二次型在 $PG_1(\mathbb{F})$中对应的二次曲面是空的；在第二种情形，它在 $PG_1(\mathbb{F})$中对应的二次曲面由两个点构成.

356

显然，秩为 2 的不可约二次型与一个可约的二次型不是射影等价，因为后者在$\mathbb{F}$上有零点而前者在$\mathbb{F}$上没有零点. 一个可约的二次型射影等价于 $x_1x_2$.

**问题 26E** 证明在特征为奇数的域$\mathbb{F}$上，一个如(26.1)的二次型是退化的，当且仅当对称矩阵 $C+C^{\mathrm{T}}$ 是奇异的. 对特征为 2 的域$\mathbb{F}$，证明 $f$ 是退化的，当且仅当 $C+C^{\mathrm{T}}$ 是奇异的且对某个满足 $f(\boldsymbol{x})=0$ 的 $\boldsymbol{x}$，$\boldsymbol{x}(C+C^{\mathrm{T}})=0$.

理解 $PG_n(\mathbb{F})$上的一个二次曲面与一个平坦面 $U$ 的交是这个平坦面上的二次曲面是重要的. 例如，假定 $U$ 是一条射影直线 $PG_1(\mathbb{F})$且 $f$ 是一个不定元为 $x_0$，$x_1$，…，$x_n$ 的二次型. $U$ 的点的齐次坐标为$\langle y\boldsymbol{a}+z\boldsymbol{b}\rangle$，这里 $\boldsymbol{a}=(a_0, a_1, \cdots, a_n)$和 $\boldsymbol{b}=(b_0, b_1, \cdots, b_n)$是线性无关向量. 这些点与 $PG_1(\mathbb{F})$的点的齐次坐标$\langle(y, z)\rangle$是一一对应的. 比如说，$f=\sum_{0\leqslant i\leqslant j\leqslant n} c_{ij}x_ix_j$，则

$$g(y,z) := \sum_{1\leqslant i\leqslant j\leqslant n} c_{ij}(ya_i + zb_i)(ya_j + zb_j)$$

是不定元为 $y$ 和 $z$ 的二次型且在 $PG_1(\mathbb{F})$中定义一个二次曲面. 二次型 $g$ 可以是退化的，即使 $f$ 不退化. 根据例 26.2，一条线或者完全包含在二次曲面 $Q$ 中，或者与 $Q$ 交于 0，1 或 2 个点.

**引理 26.4** 任何一个秩$\geqslant 3$ 的二次型 $f$ 对某个二次型 $g(x_3, \cdots, x_n)$射影等价于

$$x_1x_2+g(x_3,\cdots,x_n). \tag{26.2}$$ 357

**证明** 首先假定 $q$ 是奇数. 容易看出一个二次型 $f$ 射影等价于某个 $\sum_{1\leqslant i\leqslant j\leqslant n} c_{ij}x_ix_j$，这里 $c_{11}\neq 0$. 设 $y:=x_1+\frac{1}{2c_{11}}(c_{12}x_2+\cdots+c_{1n}x_n)$，则 $f=c_{11}y^2+g(x_2, \cdots, x_n)$. 如果 $f$ 的秩至少是 3，我们归纳地发现 $f$ 射影等价于

$$h(\boldsymbol{x})=ax_1^2+bx_2^2+cx_3^2+g'(x_4,\cdots,x_n),$$

这里 $a$，$b$，$c$ 都不等于零. 三个标量可以由任意非零的平方因子代替，并得到射影等价的一个二次型. 某一对必定相差一个平方因子，因此比如说，可以设 $b=c$.

我们断言存在 $s$，$t\in\mathbb{F}_q$ 使得 $s^2+t^2=-b^{-1}a$. 弄明白这一点的一个途径是考虑$\mathbb{F}_q$ 的加法表，这是一个拉丁方. $\mathbb{F}_q$ 中的平方数(包括 0)，有$(q+1)/2$ 个. 元素 $-b^{-1}a$(或其他任何一个元素)在由非平方元指示的拉丁方的$(q-1)/2$ 列中出现$(q-1)/2$ 次，且在由非平方元指示的拉丁方的$(q-1)/2$ 行中出现$(q-1)/2$ 次；因此，$-b^{-1}a$ 在行和列由平方元指示的子矩阵中至少出现一次. 对如此选择的 $s$ 和 $t$，$h$ 射影等价于

$$\begin{aligned}&ax_1^2+b(sx_2+tx_3)^2+b(tx_2-sx_3)^2+g'(x_4,\cdots,x_n)\\&=ax_1^2-ax_2^2-ax_3^2+g'(x_4,\cdots,x_n)\\&=(ax_1+ax_2)(x_1-x_2)-ax_3^2+g'(x_4,\cdots,x_n),\end{aligned}$$

且后者显然射影等价于(26.2).

$q$ 是偶数的情形稍为冗长，见 J. W. P. Hirschfeld(1979)中定理 5.1.7 的证明. ■

**定理 26.5** (i)任意一个秩为奇数的二次型 $f$ 对某个标量 $c$ 射影等价于

$$f_0(\boldsymbol{x}):=x_1x_2+\cdots+x_{n-2}x_{n-1}+cx_n^2. \tag{26.3}$$ 358

(ii)任意一个秩为偶数的二次型 $f$ 射影等价于

$$f_1(\boldsymbol{x}):=x_1x_2+\cdots+x_{n-3}x_{n-2}+x_{n-1}x_n \tag{26.4}$$

或者

$$f_2(\boldsymbol{x}):=x_1x_2+\cdots+x_{n-3}x_{n-2}+p(x_{n-1},x_n) \tag{26.5}$$

这里 $p(x_{n-1}, x_n)$为两个不定元的不可约二次型.

**证明** 这由引理 26.4 和归纳法得出. ■

秩为奇数的二次型(及其对应的二次曲面)称为**抛物的**. 射影等价于(26.4)的秩为偶数的二次型称为**双曲的**，与(26.5)等价的二次型称为**椭圆的**. 任意两个有给定秩的双曲二次型射影等价于(26.4)，因此彼此等价. 所有有给定偶数秩的抛物二次型是射影等价的，即我们可以在(26.3)中取 $c=1$，且所有有给定秩的椭圆二次型是射影等价的. 对此及关于典范型的更多内容，见 J. W. P. Hirschfeld(1979). 双曲二次型和椭圆二次型不是射影等价的，这是下面定理的一个结论.

**定理 26.6** 在 $PG_n(q)$中，一个非退化的二次曲面 $Q$ 有基数

$$\begin{cases}\dfrac{q^n-1}{q-1} & \text{如果 } n \text{ 是偶数,即 } Q \text{ 是抛物的,}\\ \dfrac{(q^{(n+1)/2}-1)(q^{(n-1)/2}+1)}{q-1} & \text{如果 } n \text{ 是奇数且 } Q \text{ 是双曲的,}\\ \dfrac{(q^{(n+1)/2}+1)(q^{(n-1)/2}-1}{q-1} & \text{如果 } n \text{ 是奇数且 } Q \text{ 是椭圆的.}\end{cases}$$

**证明** 一般地，如果

$$f(x_1,\cdots,x_r)=x_1x_2+g(x_3,\cdots,x_r)$$

359 且有 $N$ 个向量$(x_3,\ \cdots,\ x_r)$使得 $g(x_3,\ \cdots,\ x_r)=0$，则存在$(2q-1)N+(q-1)(q^{r-2}-N)$个向量$(x_1,\ \cdots,\ x_r)$使得 $f(x_1,\ \cdots,\ x_r)=0$. 这允许我们用归纳法验证如下的公式，这些公式给出在$\mathbb{F}_q^r$中 $r$ 个不定元的秩为 $r$ 的二次型 $f$ 的零点的个数如下：

$$\begin{cases}q^{r-1} & \text{如果 } r \text{ 是奇数,即 } f \text{ 是抛物的,}\\ q^{r-1}+q^{r/2}-q^{r/2-1} & \text{如果 } r \text{ 是偶数且 } f \text{ 是双曲的,}\\ q^{r-1}-q^{r/2}+q^{r/2-1} & \text{如果 } r \text{ 是偶数且 } f \text{ 是椭圆的.}\end{cases}$$

当然，在对应的二次曲面上 $PG_n(q)$中射影点的数目由 $r$ 换成 $n+1$，减去 1(零向量)，然后除以 $q-1$ 得到. ■

**定理 26.7** 设 $Q$ 是 $PG_n(q)$ 中非退化的二次曲面. 满足 $F\subseteq Q$ 的平坦面 $F$ 的最大射影维数是

$$\begin{cases}n/2-1 & \text{如果 } n \text{ 是奇数,即 } Q \text{ 是抛物的,}\\ (n-1)/2 & \text{如果 } n \text{ 是偶数且 } Q \text{ 是双曲的,}\\ (n-3)/2 & \text{如果 } n \text{ 是偶数且 } Q \text{ 是椭圆的.}\end{cases}$$

**证明** 设 $f$ 是一个 $r$ 个不定元的非退化二次型. 定理的陈述等价于$\mathbb{F}_q^r$的子空间 $U$ 的最大维数，使得 $f$ 在 $U$ 上消失，这个维数是

$$\begin{cases}(r-1)/2 & \text{如果 } r \text{ 是奇数,即 } f \text{ 是抛物的,}\\ r/2 & \text{如果 } r \text{ 是偶数且 } f \text{ 是双曲的,}\\ r/2-1 & \text{如果 } r \text{ 是偶数且 } f \text{ 是椭圆的.}\end{cases}$$

首先注意到，如果 $f$ 等于(26.3)中的 $f_0$，则对任意的 $\boldsymbol{x}\in\mathrm{span}(\boldsymbol{e}_2,\ \boldsymbol{e}_4,\ \cdots,\ \boldsymbol{e}_{r-1})$，$f(\boldsymbol{x})=0$，这里 $\boldsymbol{e}_1,\ \boldsymbol{e}_2,\ \cdots,\ \boldsymbol{e}_r$ 是$\mathbb{F}_q^r$的标准基. 如果 $f$ 等于(26.4)中的 $f_1$，则对任意的 $\boldsymbol{x}\in\mathrm{span}(\boldsymbol{e}_2,\ \boldsymbol{e}_4,\ \cdots,\ \boldsymbol{e}_r)$，$f(\boldsymbol{x})=0$. 如果 $f$ 等于(26.5)中的 $f_2$，则对任意的 $\boldsymbol{x}\in\mathrm{span}(\boldsymbol{e}_2,\ \boldsymbol{e}_4,\ \cdots,\ \boldsymbol{e}_{r-2})$，$f(\boldsymbol{x})=0$. 这些空间的维数分别是$(r-1)/2$，$r/2$ 和 $r/2-1$.

剩下的尚需证明，对这些情形中的任意一种，$f$ 在维数较大的空间上不为零. 我们将利用

360 定理 26.5 和归纳法进行证明. $r=1$ 和 $r=2$ 的情形是平凡的. 假设 $f(x_1,\ \cdots,\ x_r)=x_1x_2+g(x_3,\ \cdots,\ x_r)$且对某个 $k$ 维子空间 $U\subseteq\mathbb{F}_q^r$的所有 $\boldsymbol{x}$，$f(\boldsymbol{x})=0$. 为了完成证明，需要证明存在维数$\geqslant k-1$ 的一个子空间$U'\subseteq\mathbb{F}_q^{r-2}$使得对所有 $y\in U'$，$g(\boldsymbol{y})=0$.

显然，对所有在

$$U_0:=\{(x_3,\cdots,x_r):(0,0,x_3,\cdots,x_r)\in U\}$$

中的 $\boldsymbol{y}$，$g(\boldsymbol{y})=0$. 如果 $\dim(U_0)\geqslant k-1$，我们就完成了证明，因此假设 $\dim(U_0)=k-2$. 则

存在 $U$ 中的向量

$$(1,0,a_3,\cdots,a_r) \quad 和 \quad (0,1,b_3,\cdots,b_r).$$

于是$(1, 1, a_3+b_3, \cdots, a_r+b_r)\in U$，因此 $g(a_3+b_3, \cdots, a_r+b_r)=-1$. 显然，二次型 $g$ 在

$$\text{span}((a_3,\cdots,a_r))+U_0 \quad 和 \quad \text{span}((b_3,\cdots,b_r))+U_0$$

中的所有向量上为零. 这些子空间中之一一定有$>k-2$ 的维数，因为否则$(a_3+b_3, \cdots, a_r+b_r)\in U_0$，这与 $g(a_3+b_3, \cdots, a_r+b_r)=-1$ 矛盾. ■

**例 26.3** 设 $f$ 为三个不定元的二次型，并在射影平面 $PG_2(q)$上考虑二次曲面 $Q(f)$. 如果 $f$ 非退化，则 $Q(f)$有 $q+1$ 个射影点. 如前面所说，$PG_2(q)$的任意一条线 $L$ 交 $Q(f)$于 $L$ 上的一个二次曲面，在这一情形两者有 0，1 或 2 个交点，因为由定理 26.7，$Q(f)$不能包含 $L$. 于是 $Q(f)$是 $q+1$ 个点的集合，其中没有三点共线，即 $Q(f)$是一个卵形，见问题 19I.

如果 $f$ 的秩为 0，则 $Q(f)$是 $PG_2(q)$中的所有点. 如果 $f$ 的秩为 1，$Q(f)$由 $PG_2(q)$中的一条线上的点构成. 如果 $f$ 的秩为 2，有两种情形：如果 $f$ 可约，比如说 $f$ 射影等价于 $xy$，则$Q(f)$由在 $PG_2(q)$的两条线的并中的点组成；如果 $f$ 不可约，则 $Q(f)$是 $PG_2(q)$中的单独一个点.

**例 26.4** 一阶里德-米勒码已在第 18 章引入. 这里是引入整个族的一种方式：设 $V=\mathbb{F}_2^m$. 我们考虑其坐标由 $V$ 的元素指示的长度为 $2^m$ 的向量；为了具体，写成 $V=\{\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{2^m-1}\}$. *$k$ 阶里德-米勒码* $RM(k, m)$定义成(长度为 $2^m$ 的)所有向量 [361]

$$(f(\boldsymbol{v}_0),f(\boldsymbol{v}_1),\cdots,f(\boldsymbol{v}_{2^m-1})),$$

这里 $f$ 遍历 $x_1, \cdots, x_m$ 的次数至多为 $k$ 的所有多项式.

因为在$\mathbb{F}_2$上线性型 $x_{i_1}+\cdots+x_{i_k}$与二次型 $x_{i_1}^2+\cdots+x_{i_k}^2$ 给出同一函数，二阶码 $RM(2, m)$中的字由二元二次型 $f(x_1, \cdots, x_n)$及它们的“补”$f(x_1, \cdots, x_n)+1$ 给出. 定理 26.4 和定理 26.5 对确定发生在 $RM(2, m)$中码字的重量是有用的.

我们也要考虑退化的情形，例如 $x_1x_2+x_3x_4$ 对应 $RM(2, 6)$中重量为 24 的一个码字. 可以发现 $RM(2, 6)$中码字的重量是 0，16，24，28，32，36，40，48 和 64.

**问题 26F** 设 $f(\boldsymbol{x}) := x_1x_2+\cdots+x_{2m-1}x_{2m}$. 在由对应于 $f(\boldsymbol{x})+a(\boldsymbol{x})$的字组成的 $RM(2, 2m)$中，则 $f$ 确定了$RM(1, 2m)$的一个陪集 $C$，这里 $a(\boldsymbol{x})$遍历 $2m$ 个变量的 $2^{2m+1}$个仿射函数(线性函数加上一个可能的常数项). 证明在 $C$ 中一半字的重量为 $2^{2m-1}+2^{m-1}$，另一半字的重量为 $2^{2m-1}-2^{m-1}$.

**例 26.5** 设 $Q_3$ 是射影 3-空间 $PG_3(q)$上的一个非退化的椭圆二次曲面. 由定理 26.6，$|Q_3|=q^2+1$. 由定理 26.7，$Q_3$ 不包含直线. 任意一个平面 $P$ 交 $Q_3$ 于那个平面上的一个二次曲面；根据例 26.3，每个平面与 $Q_3$ 交于这个平面上的一个卵形或者单独一个点. $Q_3$ 的任意三个点包含在唯一一个平面中，因此得出平面与 $Q_3$ 的非平凡的交可为施泰纳系

$$S(3,q+1,q^2+1)$$

提供区组. 一般地，在 $PG_3(q)$上没有三点共线的 $q^2+1$ 个点的集合称为*卵形面*，$S(3, n+1, n^2+1)$称为*默比乌斯平面*或*反演平面*.

**例 26.6**　设 $Q_4$ 是射影 4-空间 $PG_4(q)$上的一个非退化的二次曲面. 由定理 26.6，$|Q_4|=q^3+q^2+q+1$. 设$\mathcal{Q}$为关联结构，其点是 $Q_4$ 的元素，区组是 $PG_4(q)$中完全被 $Q_4$ 包含的线. $\mathcal{Q}$的每个点恰好在$\mathcal{Q}$的 $q+1$ 个区组中(见问题 26F). 给定$\mathcal{Q}$的一个点 $x$ 和一个区组 $L$，平面 $P:=\{x\}\vee L$ 与 $Q_4$ 的交是 $P$ 中的一个二次曲面 $Q_2$，显然，$Q_2$ 包含一条线和不在这条线上的一个点. 由例 26.3，$Q_2$ 一定由在两条(相交的)线上的点组成. 这蕴涵$\mathcal{Q}$是一个部分几何 $pg(r,k,t)$，如在第 21 章定义的，这里

$$r=q+1,k=q+1,t=1.$$

**例 26.7**　设 $Q_5$ 为 $PG_5(q)$上的一个非退化的椭圆二次曲面. 由定理 26.6，$|Q_5|=(q+1)(q^3+1)$. 由定理 26.7，$Q_5$ 不包含平面. 设$\mathcal{Q}$为关联结构，其点为 $Q_5$ 的元素且其区组为完全包含在 $Q_5$ 中的 $PG_5(q)$的线. 由问题 26F，$\mathcal{Q}$的每个点在$\mathcal{Q}$的 $q^2+1$ 条线上. 由类似于例 26.6 的论证，$\mathcal{Q}$是一个部分几何 $pg(r,k,t)$，这里

$$r=q^2+1,k=q+1,t=1.$$

$t=1$ 的部分几何称为广义四边形. 进一步的结果和参考书见 L. M. Batten(1986).

**问题 26G**　设 $f$ 为$\mathbb{F}_q$ 上有 $n$ 个不定元的一个非退化二次型，如在(26.1)中由一个矩阵 $C=(c_{ij})$所给出的. 设 $Q=Q(f)$是 $PG_{n-1}(\mathbb{F}_q)$中对应的二次曲面. 设 $p=\langle x\rangle$是 $Q$ 上的一个点. 设

$$T_p:=\{\langle \boldsymbol{y}\rangle:\boldsymbol{x}(C+C^{\top})\boldsymbol{y}^{\top}=0\}.$$

则由问题 26E，$T_p$ 是 $PG_{n-1}(\mathbb{F}_q)$中的超平面. 证明 $T_p\cap Q$ 恰由 $p$ 和含于 $Q$ 中的 $p$ 上的直线的并组成. 进一步证明，如果 $W$ 为 $T_p$ 中不包含 $p$ 的任意一个超平面，则 $Q':=W\cap Q$ 是 $W(=PG_{n-3}(\mathbb{F}_q))$中的一个非退化二次曲面，且 $Q'$根据 $Q$ 是抛物的、双曲的或椭圆的而是抛物的、双曲的或椭圆的. 特别地，我们看到 $p$ 上完全位于 $Q$ 中的线的数目是 $|Q'|$.

$\mathbb{F}_{q^2}$ 上的一个埃尔米特型是形如

$$h(\boldsymbol{x})=h(x_1,\cdots,x_n)=\sum_{i,j=1}^{n}c_{ij}x_ix_j^q \tag{26.6}$$

的表达式，这里系数 $c_{ij}$ 来自$\mathbb{F}_{q^2}$ 且 $c_{ji}=c_{ij}^q$. 特别地，对角系数 $c_{ii}$ 由弗罗贝尼乌斯自同构$x\mapsto x^q$ 固定，位于$\mathbb{F}_q$ 中.

$\mathbb{F}_{q^2}$ 上的两个埃尔米特型是射影等价的，如果 $g$ 能从 $f$ 由一个可逆线性替换得到，或者用矩阵的记号，对$\mathbb{F}_{q^2}$ 上的某个非奇异矩阵 $A$，$g(\boldsymbol{x})=f(\boldsymbol{x}A)$. 于是，如果 $f$ 由一个矩阵 $C$ 定义，如同在(26.6)中，即 $f(\boldsymbol{x})=\boldsymbol{x}C\boldsymbol{x}^{\top}$，则 $g$ 由矩阵 $ACA^*$ 定义，这里 $A^*$ 是 $A$ 的共轭转置；如果 $A=(a_{ij})$，则 $A^*:=(a_{ji}^q)$.

一个埃尔米特型的秩是在所有射影等价的埃尔米特型中出现的不定元(系数非零)的最小个数.

在 $PG_n(q^2)$中，一个埃尔米特簇是射影点的集合

$$H=H(f):=\{\langle \boldsymbol{x}\rangle:f(\boldsymbol{x})=0\},$$

这里 $f$ 是有 $n+1$ 个不定元的埃尔米特型，为了作出这个定义，我们一定要选择一组基并将向量与$\mathbb{F}_{q^2}$ 上的$(n+1)$元组等同起来. 可以看到一个埃尔米特簇在 $PG_n(q^2)$中与一个平坦面的交是这个平坦面中的一个埃尔米特簇.

**定理 26.8**　一个秩为 $n$ 的埃尔米特型射影等价于

$$x_1^{q+1}+x_2^{q+1}+\cdots+x_n^{q+1}. \tag{26.7}$$

**证明** 不难看出，任意一个非零的埃尔米特型射影等价于如(26.6)中的 $h$，这里 $c_{11}\neq 0$；这留给读者证明．设 $y:=c_{11}x_1+c_{12}x_2+\cdots+c_{1n}x_n$．则 $h=c_{11}^{-1}yy^q+g(x_2,\cdots,x_n)$，这里 $g$ 是一个不定元为 $x_2,\cdots,x_n$ 的埃尔米特型．因为 $c_{11}\in\mathbb{F}_q$，存在 $a\in\mathbb{F}_{q^2}$ 使得 $a^{q+1}=c_{11}^{-1}$，则 $h=z^{q+1}+g(x_2,\cdots,x_n)$，这里 $z=ay$.

由这一步和归纳法得出本定理. ■ [364]

**定理 26.9** *在 $PG_n(q^2)$ 中，一个非退化的埃尔米特簇 $H$ 的点的数目是*

$$\frac{(q^{n+1}+(-1)^n)(q^n-(-1)^n)}{q^2-1}.$$

**证明** 对每个非零的 $a\in\mathbb{F}_q$，存在 $x\in\mathbb{F}_{q^2}$ 的 $q+1$ 个值，使得 $x^{q+1}=a$．如果

$$f(x_1,\cdots,x_n)=x_1^{q+1}+g(x_2,\cdots,x_n)$$

且有 $N$ 个向量 $(x_2,\cdots,x_n)$ 使得 $g(x_2,\cdots,x_n)=0$，则存在 $N+(q+1)(q^{2(n-1)}-N)$ 个向量 $(x_1,\cdots,x_n)$ 使得 $f(x_1,\cdots,x_n)=0$．由归纳法，存在 $q^{2n-1}+(-1)^n(q^n-q^{n-1})$ 个 $\mathbb{F}_{q^2}^n$ 中的向量是(26.7)的零点，得出定理. ■

**例 26.8** 在射影直线 $PG_1(q^2)$ 中考虑埃尔米特簇．如果一个有两个不定元的埃尔米特型的秩为 0，则簇 $H(f)$ 包含所有 $q^2+1$ 个点；如果 $f$ 的秩为 1，则 $H(f)$ 由一个点构成；如果 $f$ 的秩为 2，则 $H(f)$ 包含 $q+1$ 个点．由此得出，对任意 $n$，如果 $H$ 是 $PG_n(q^2)$ 中的一个埃尔米特簇，则 $PG_n(q^2)$ 的线交 $H$ 于 1，$q+1$ 或 $q^2+1$ 个点.

现在考虑射影平面 $PG_2(q^2)$ 中的一个非退化的埃尔米特簇 $H_2$．由定理 26.9，它有 $q^3+1$ 个点．任意一条线 $L$ 交 $H_2$ 于这条线上的一个埃尔米特簇 $L\cap H_2$．作为一个练习，读者应检验没有线包含在 $H_2$ 中，因此 $|L\cap H_2|=1$ 或 $q+1$．由此得出 $PG_2(q^2)$ 的线与 $H_2$ 的非平凡交为点集 $H_2$ 上的施泰纳系

$$S(2,q+1,q^3+1)$$

提供区组.

具有这些参数的设计称为*单元*．进一步的分析证明上面构造的设计是可分解的，见 R. C. Bose(1959).

我们通过构造例 26.5 中施泰纳系 $S(3,q+1,q^2+1)$ 的高维类似结束本章，以下这些设计曾被称为*圆几何*. [365]

**定理 26.10** *如果 $q$ 是一个素数的幂且 $n$ 为一个正整数，则存在施泰纳系 $S(3,q+1,q^n+1)$.*

**证明** 设 $V$ 是 $\mathbb{F}_{q^n}$ 上的一个 2 维向量空间且设 $\mathcal{X}$ 为 $V$ 在 $\mathbb{F}_{q^n}$ 上的 1 维子空间的集合(即 $PG_1(q^n)$ 的 $q^n+1$ 个点，阶为 $q^n$ 的射影线).

现在把 $V$ 看成 $\mathbb{F}_q$ 上的 $2n$ 维向量空间．我们要构造的施泰纳系的区组来自 $V$ 中 $\mathbb{F}_q$ 上的 2 维子空间 $U$，$U$ 不包含 $\mathcal{X}$ 的任何一个成员．对每一个这样的 $U$，设

$$B_U:=\{P\in\mathcal{X}:P\cap U\neq\{\mathbf{0}\}\}.$$

注意每个 $P\in B_U$ 交 $U$ 于 $\mathbb{F}_q$ 上的一个 1 维子空间(它包含 $U$ 的 $q^2-1$ 个非零向量中的 $q-1$ 个向量)，因此 $|B_U|=q+1$．如果对某个非零的标量 $\lambda\in\mathbb{F}_{q^n}$，$W=\lambda U$，则 $B_U=B_W$，我们只取不

同的集合 $B_U$ 作为区组.

考虑三个不同的点 $P_i\in\mathcal{X}$，$i=1$，2，3. 比如说 $P_i$ 是向量 $\boldsymbol{x}_i$ 的$\mathbb{F}_{q^n}$-生成，$i=1$，2，3. 这三个向量在$\mathbb{F}_{q^n}$上是线性相关的，设为

$$\boldsymbol{x}_3=\alpha\boldsymbol{x}_1+\beta\boldsymbol{x}_2,$$

这里 $\alpha$，$\beta\in\mathbb{F}_{q^n}$. 那么 $U:=\mathrm{Span}_{\mathbb{F}_q}\{\alpha\boldsymbol{x}_1,\beta\boldsymbol{x}_2\}$ 与 $P_1$，$P_2$ 和 $P_3$ 非平凡地相交是显然的. 假设 $\mathbb{F}_q$ 上的某个 2 维子空间 $W$ 与每个 $P_i$ 非平凡地相交，比如说 $W$ 包含 $\gamma_i\boldsymbol{x}_i$，$0\neq\gamma_i\in\mathbb{F}_{q^n}$，$i=1$，2，3. 则这些向量在$\mathbb{F}_q$上是线性相关的，设为

$$\gamma_3\boldsymbol{x}_3=a\gamma_1\boldsymbol{x}_1+b\gamma_2\boldsymbol{x}_2,$$

这里 $a$，$b\in\mathbb{F}_q$. 因为 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 在$\mathbb{F}_{q^n}$上是线性无关的，我们有 $\gamma_3\alpha=a\gamma_1$，且 $\gamma_3\beta=b\gamma_2$. 由此 $\gamma_3U=W$，我们看到三个不同的点包含在唯一一个区组中. ■

**问题 26H** 设 $\alpha$ 是射影平面 $\boldsymbol{P}$ 的一个直射变换.

366 (i)证明：如果 $\alpha$ 固定一条线 $l$ 上的所有点和两个不在 $l$ 上的点，则 $\alpha$ 逐点固定 $\boldsymbol{P}$.

(ii)如果 $\alpha$ 固定一条线 $l$ 上的所有点，则存在一个点 $P$ 使得 $\alpha$ 固定 $P$ 和每条通过 $P$ 的线.

($\boldsymbol{P}$ 的这样一个自同构称为*中心直射变换*.)

**问题 26I** 在第 23 章中，我们看到 $AG(3,q)$是 $PG(3,q)$的一个子几何，这里缺失的部分是一个射影平面 $P$，有时称之为 $AG(3,q)$的*无穷远平面*. 设 $q=2^m$ 且设 $O$ 为 $P$ 上的一个超卵形. 我们以 $AG(3,q)$的点作为点，$AG(3,q)$与 $P$ 交于 $O$ 的一个点的线作为线，定义一个关联结构 $\boldsymbol{I}$. 证明 $\boldsymbol{I}$ 是一个广义四边形.

**问题 26J** 考虑 $PG(2,4)$中的一个超卵形 $O$. 定义一个图 $G$，$G$ 的顶点是该平面上不在 $O$ 中的点，边为$(x,y)$，如果通过 $x$ 和 $y$ 的线与 $O$ 相交. 证明：

(i)每条边在唯一的一个三角形中.

(ii)对每个三角形$(x,y,z)$，所有其他的点恰与 $x$，$y$，$z$ 中的一个相连.

(iii)$G$ 是一个广义四边形.

**问题 26K** 考虑任意一个对称$(v,k,\lambda)$-设计，定义*弧*是一个点集 $S$，使没有三个点在一个区组中. 区组称为 $S$ 的*切线*，如果它与 $S$ 交于一个点. 依据 $S$ 是否有切线找出 $|S|$ 的一个上界.

**问题 26L** 一个对称设计中的*卵形*是满足问题 26J 中的界的一条弧. 考虑参数为$(4\lambda-1,2\lambda,\lambda)$的一个对称设计，证明这个设计中的卵形是其补设计中规模为 3 的线.

## 评注

术语"最大$(m,k)$-弧"在文献中常用于我们所说的"完全的$(m,k)$-弧"，但这里我们不用"最大".

在 D. K. Ray-Chaudhuri(1962)以及 R. C. Bose and I. M. Chakravarti(1966)中更详细地讨论了二次曲面和埃尔米特簇的性质.

367 定理 26.3 的证明中描述的多项式方法有进一步的应用. 例如，A. Blokhuis(1994)证明了 J. di Paola 的一个猜想：$PG(2,p)$中的一个非平凡区组化集至少有$(3p+1)/2$ 个点. 证明思路

是注意区组化集 $S$ 一定有一条切线，不失一般性，切线是无穷远线. 设在该仿射平面上的其他点为$(a_i, b_i)$，$i=1, \cdots, p+k$. 关于多项式

$$F(t,u) = \prod_{i=1}^{p+k}(t + a_i + ub_i)$$

的复杂研究可以证明 $k \geqslant \frac{p+1}{2}$.

## 参考文献


L. M. Batten (1986), *Combinatorics of Finite Geometries*, Cambridge University Press.

A. Blokhuis (1994), On the size of a blocking set in $PG(2,p)$, *Combinatorica* **14** (1994), 111–114.

R. C. Bose (1959), On the application of finite projective geometry for deriving a certain series of balanced Kirkman arrangements, *Golden Jubilee Commemoration Volume (1958–59)*, Calcutta Math. Soc., pp. 341–354.

R. C. Bose and I. M. Chakravarti (1966), Hermitian varieties in a finite projective space $PG(N,q^2)$, *Canad. J. Math* **18**, 1161–1182.

A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combinatorial Theory* (A) **24** (1978), 251–253.

P. Dembowski (1968), *Finite Geometries*, Springer-Verlag.

R. H. F. Denniston (1969), Some maximal arcs in finite projective planes, *J. Combinatorial Theory* **6**, 317–319.

J. W. P. Hirschfeld (1979), *Projective Geometries over Finite Fields*, Clerendon Press.

D. K. Ray-Chaudhuri (1962), Some results on quadrics in finite projective geometry based on Galois fields, *Canad. J. Math.* **14**, 129–138.


368

# 第27章 差集和自同构

一类对称设计起源于交换群中的差集(在下面定义). 这样的一个设计出现在例19.6中，该群重新出现在这个设计的自同构群中.

在一个简单的关联结构中，我们可以等同区组与点集，即区组集$\mathcal{A}$是点集$X$的子集族，对称设计$(X,\mathcal{A})$或任何简单的关联结构的自同构是$X$的一个置换$\alpha$，它把$\mathcal{A}$带到$\mathcal{A}$，即对$A\subseteq X$，$A\in\mathcal{A}$当且仅当$\alpha(A)\in\mathcal{A}$. 下面首先讨论关于一般对称设计的自同构的一个定理.

**定理 27.1** 设$\mathcal{S}=(X,\mathcal{A})$是一个对称$(v,k,\lambda)$-设计且$\alpha$是$\mathcal{S}$的一个自同构. 则在$\alpha$下不动点的数目等于在$\alpha$下不动区组的数目.

**证明** 设$N$为$\mathcal{S}$的关联矩阵，定义一个置换矩阵$P$，它的行和列由点指示且这里

$$P(x,y):=\begin{cases}1 & \text{如果 } \alpha(x)=y,\\ 0 & \text{否则.}\end{cases}$$

定义一个置换矩阵$Q$，它的行和列由区组指示且这里

$$Q(A,B):=\begin{cases}1 & \text{如果 } \alpha(A)=B,\\ 0 & \text{否则.}\end{cases}$$

369

注意$P$的迹等于不动点的数目，且$Q$的迹等于$\alpha$的不动区组的数目.

现在我们有

$$\begin{aligned}PNQ^{\top}(x,A)&=\sum_{y\in X,B\in\mathcal{A}}P(x,y)N(y,B)Q(A,B)\\&=N(\alpha(x),\alpha(A))=N(x,A).\end{aligned}$$

这就是说，$PNQ^{\top}=N$. 等价地，$P=NQN^{-1}$. $P$和$Q$由于是相似矩阵，因此有相同的迹，定理得证. ■

**推论** 点集$X$上$\alpha$的圈分解的类型与区组集$\mathcal{A}$上$\alpha$的圈分解的类型相同.

**证明** 由定理27.1，对每个$i=1,2,\cdots$，$\alpha^i$的不动点的数目与其不动区组的数目相同.

假设在某个集合$S$上，一个置换$\beta$有长度$i$的圈$c_i$，$i=1,2,\cdots,|S|$. 设$f_j$表示$\beta^j$的不动点的数目，则

$$f_j=\sum_{i|j}ic_i,$$

由默比乌斯反演，即定理10.4，

$$jc_j=\sum_{i|j}\mu\left(\frac{j}{i}\right)f_i.$$

要点是每个长度的圈的数目(即$\beta$的类型)完全由$\beta$的幂的不动点的数目确定. ■

**推论** 如果$\Gamma$是一个对称设计的自同构群，则点集$X$上$\Gamma$的轨道数与区组集$\mathcal{A}$上$\Gamma$的轨道数相同. 特别地，$\Gamma$在点上是传递的当且仅当$\Gamma$在区组上是传递的.

**证明** 由伯恩赛德引理，即定理 10.5，集合 $S$ 的一个置换群 $\Gamma$ 的轨道数恰好由多重集 $(f(\alpha):\alpha\in\Gamma)$确定，这里 $f(\alpha)$是 $\alpha$ 下 $S$ 的不动元素数. ■ [370]

在介绍差集之前，我们先给出关于任意 2-设计的自同构群的轨道的定理. 这个定理称为布洛克(Block)引理，见 Block(1967). 这为上面的推论提供了另一个证明，因为按照定理 19.9，一个对称设计的对偶也是一个 2-设计.

**定理 27.2** 如果 $\Gamma$ 是满足 $v>k$ 的 2-$(v, k, \lambda)$设计的自同构群，则 $\Gamma$ 在点集 $X$ 上的轨道数小于或等于 $\Gamma$ 在区组集 $\mathcal{A}$ 上的轨道数.

**证明** 设 $X_1, X_2, \cdots, X_s$ 是 $X$ 上 $\Gamma$ 的轨道且 $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_t$ 为 $\mathcal{A}$ 上 $\Gamma$ 的轨道. 定义两个 $s\times t$ 矩阵 $C$, $D$ 如下. $C(i, j)$是与一个不动区组 $A\in\mathcal{A}_j$ 关联的点 $x\in X_i$ 的数目(这个数对 $\mathcal{A}_j$ 中的任何一个区组 $A$ 都是相同的). $D(i, j)$是与一个不动点 $x\in X_i$ 关联的区组 $A\in\mathcal{A}_j$ 的数目(这个数对 $X_i$ 中的任意一点 $x$ 都是相同的).

考虑 $s\times s$ 矩阵积 $CD^\top$. $CD^\top(i, \ell)$是有序对$(x, A)\in X_i\times\mathcal{A}_j$ 的数目对所有 $j$ 求和，这里 $x$ 与 $A$ 关联且 $A$ 与 $X_\ell$ 中的一个不动点 $y$ 关联. 因此，如果 $i\neq\ell$，$CD^\top(i, \ell)=\lambda|X_i|$，且$CD^\top(i, i)=(r-\lambda)+\lambda|X_i|$；这就是，

$$CD^\top=(r-\lambda)I+\lambda\operatorname{diag}(|X_1|,|X_2|,\cdots,|X_s|)J.$$

这与矩阵等式(19.7)类似. 因为 $v>k$，我们有 $r>\lambda$ 且右端的矩阵可以由几种方式看出它是非奇异的，例如计算其行列式. 由此得出 $C$(及 $D$)的秩为 $s$，$s$ 不能超过列数 $t$. ■

* * *

设 $G$ 为一个 $v$ 阶交换群. $G$ 中的一个$(v, k, \lambda)$-差集是 $k$-子集 $D\subseteq G$，使得每个非零的 $g\in G$在 $D$ 的差的多重集$(x-y:x, y\in D)$中恰出现 $\lambda$ 次. 更正式一些，我们要求 $g\neq 0$ 时满足 $x, y\in D$ 且 $x-y=g$ 的有序对$(x, y)$的数目是 $\lambda$，且当 $g=0$ 时这个数目为 $k$，显然，$\lambda(v-1)=k(k-1)$. [371]

**例 27.1** 差集的例子包括：

$(7,3,1)$ $\{1,2,4\}$ 在$\mathbb{Z}_7$ 中

$(13,4,1)$ $\{0,1,3,9\}$ 在$\mathbb{Z}_{13}$中

$(11,5,2)$ $\{1,3,9,5,4\}$ 在$\mathbb{Z}_{11}$中

$(16,6,2)$ $\{10,20,30,01,02,03\}$ 在 $\mathbb{Z}_4\times\mathbb{Z}_4$ 中

$(16,6,2)$ $\{0000,0001,0010,0100,1000,1111\}$ 在$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$中

当 $1<k<v-1$ 时差集是非平凡的. $\lambda=1$ 的差集有时称为平面的或简单的.

设 $G$ 为 $v$ 阶交换群. 对 $S\subseteq G$, $g\in G$，我们用 $S+g$ 表示由 $g$ 产生的 $S$ 的平移或迁移

$$S+g:=\{x+g:x\in S\}.$$

设 $D$ 为$G$ 的一个 $k$-子集且 $x, y\in G$. 一般地，我们断言既包含 $x$ 又包含 $y$ 的迁移 $D+g$ 的数目等于作为 $D$ 中差 $d:=x-y$ 出现的次数. 这是因为 $g\mapsto(x-g, y-g)$是集合$\{g\in G:\{x, y\}\subseteq D+g\}$和 $D$ 中的元素使得 $a-b=x-y$ 的有序对$(a, b)$的集合之间的一一对应.(读者可以检验这个公共数目也等于交$(D+x)\cap(D+y)$的基数.)

特别地，$(G, \{D+g:g\in G\})$是一个对称的$(v, k, \lambda)$-设计当且仅当 $D$ 是一个$(v, k, \lambda)$-

差集.

**问题 27A** $v$ 阶任意群 $G$ 中的 $(v, k, \lambda)$-商集(写成乘法)是一个 $k$-子集 $D\subseteq G$,使得下述条件之一成立:

(1)每个非单位元元素 $g\in G$ 在出自 $D$ 的"右"商的表 $(xy^{-1}: x, y\in D)$ 中恰出现 $\lambda$ 次.

(2)每个非单位元元素 $g\in G$ 在出自 $D$ 的"左"商的表 $(x^{-1}y: x, y\in D)$ 中恰出现 $\lambda$ 次.

(3)对每个非单位元元素 $g\in G$, $|D\cap(Dg)|=\lambda$.

(4)对每个非单位元元素 $g\in G$, $|D\cap(gD)|=\lambda$.

(5) $(G, \{Dg: g\in G\})$ 是一个对称 $(v, k, \lambda)$-设计.

(6) $(G, \{gD: g\in G\})$ 是一个对称 $(v, k, \lambda)$-设计.

证明以上六个条件是等价的.

372

**定理 27.3** 设 $G$ 为一个 $v$ 阶的群,在 $G$ 中存在一个 $(v, k, \lambda)$-商集等价于存在自同构群 $\hat{G}$ 的一个对称 $(v, k, \lambda)$-设计,$\hat{G}$ 同构于 $G$ 且在该设计的点上是正则的,即精确传递的.

**证明** 设 $D$ 为 $G$ 中的一个 $(v, k, \lambda)$-商集,则 $(G, \{gD: g\in G\})$ 是一个对称 $(v, k, \lambda)$-设计. 对 $g\in G$,用 $\hat{g}(x)=gx$ 定义 $G$ 的一个置换 $\hat{g}$,则每个 $\hat{g}$ 事实上是 $(G, \{gD: g\in G\})$ 的一个自同构,而自同构群 $\hat{G}=\{\hat{g}: g\in G\}$ 显然同构于 $G$ 且在该设计的点上是正则的.

反之,设给定 $G$ 且设 $(X, \mathcal{A})$ 为一个对称 $(v, k, \lambda)$-设计,使它具有 $(X, \mathcal{A})$ 的自同构正规群 $\hat{G}$,这里 $\hat{G}$ 同构于 $G$. 在 $\hat{G}$ 中展示一个 $(v, k, \lambda)$-商集就够了.

固定一个点 $x_0\in X$ 和一个区组 $A_0\in\mathcal{A}$. 设

$$D:=\{\sigma\in\hat{G}: \sigma(x_0)\in A_0\}.$$

我们断言 $D$ 是 $\hat{G}$ 中的一个 $(v, k, \lambda)$-商集. 因为 $\hat{G}$ 是正则的且 $|A_0|=k$,我们有 $|D|=k$. 设 $\alpha$ 是 $\hat{G}$ 的一个非单位元元素. 则 $\alpha D=\{\alpha\sigma: \sigma(x_0)\in A_0\}=\{\tau: \tau(x_0)\in\alpha(A_0)\}$,因此

$$D\cap(\alpha D)=\{\tau: \tau(x_0)\in A_0\cap\alpha(A_0)\}.$$

因为 $\hat{G}$ 是正则的,$\alpha$ 没有不动点,且因此由定理 27.1,不使任何区组不动. 于是区组 $\alpha(A_0)$ 与 $A_0$ 不同,所以 $|A_0\cap\alpha(A_0)|=\lambda$,再由正则性 $|D\cap(\alpha D)|=\lambda$. 这对所有的非单位元元素成立并建立了我们的断言. ■

特别地,一个循环 $(v, k, \lambda)$-差集,即 $\mathbb{Z}_v$ 中的一个差集的存在性等价于有循环自同构的一个对称 $(v, k, \lambda)$-设计的存在性,一个循环自同构是这样的自同构,即点或区组上的圈分解仅由长度为 $v$ 的一个圈构成.

现在讨论交换群中的差集. 理想地,我们想描述所有的差集并给它们分类——找出哪些群有差集,有多少,等等. 我们对各种较小的参数三元组这样来做,但一般来说仅存在性问题已极为困难.

373

观察到 $D\subseteq G$ 是一个 $(v, k, \lambda)$-差集,当且仅当 $G\setminus D$ 是一个 $(v, v-k, v-2k+\lambda)$-差集. 因此我们讨论 $k<\frac{1}{2}v$ 的情形.

还注意到 $D$ 是差集当且仅当 $D$ 的每个平移是一个差集.

在$(v, k)=1$的情形，我们可以从所有平移的类中选择一个自然的表示，这有助于分类且在下一章有用. 称交换群$G$的一个子集是正规化的，如果它的所有元素之和是零.

**命题 27.4** 设$D$是$v$阶交换群$G$的一个$k$-子集. 如果$(v, k)=1$，则$D$有一个唯一的正规化平移.

**证明** 设$h$为$D$的元素之和. 则一个平移$D+g$的元素之和是$h+kg$. 因为$(v, k)=1$，存在一个唯一的群元素$g$满足$h+kg=0$. ■

请读者按自己的满意度验证参数$(v, k, \lambda)=(7, 3, 1)$，$(13, 4, 1)$，$(11, 5, 2)$，$(21, 5, 1)$的正规化差集分别是

$\{1,2,4\},\{3,5,6\}$ 在$\mathbb{Z}_7$ 中；

$\{0,1,3,9\},\{0,2,5,6\},\{0,4,10,12\},\{0,7,8,11\}$ 在$\mathbb{Z}_{13}$中；

$\{1,3,4,5,9\},\{2,6,7,8,10\}$ 在$\mathbb{Z}_{11}$中；

$\{7,14,3,6,12\},\{7,14,9,15,18\}$ 在$\mathbb{Z}_{21}$中.

(这在定理 28.3 之后是容易的，见例 28.2.)当然，当$(v, k)=1$时，差集的总数是$v$乘以正规化差集的数目，例如，在$\mathbb{Z}_{13}$中，参数为$(13, 4, 1)$的差集有 52 个.

最后一个初等观察是，如果$\alpha$是群$G$的任何一个自同构，则子集$D\subseteq G$是一个差集当且仅当$\alpha(D)$是一个差集. 因此，从一个差集可以通过平移以及由$G$的对称性得到其他差集. 我们说$G$中的两个差集$D_1$，$D_2$是等价的，如果存在$\alpha\in \mathrm{Aut}(G)$和$g\in G$使得$D_2=\alpha(D_1)+g$.（检验这是一个等价关系.）上面对参数的每个三元组给出的正规化差集是等价的，事实上，每一个差集可以从其他差集通过乘以一个与各自的群的阶互素的某个整数得到. [374]

**问题 27B** 证明在$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$中，所有$(16, 6, 2)$-差集是等价的.

**问题 27C** 由例 19.4 回忆与正则阿达马矩阵相关的参数为$v=4t^2$，$k=2t^2-t$，$\lambda=t^2-t$的对称设计. 设$A$和$B$分别是群$G$和$H$中的$(4x^2, 2x^2-x, x^2-x)$-差集和$(4y^2, 2y^2-y, y^2-y)$-差集(准许$x$或$y=1$). 证明

$$D := (A\times(H\setminus B))\cup((G\setminus A)\times B)$$

是群$G\times H$中的一个$(4z^2, 2z^2-z, z^2-z)$-差集，这里$z=2xy$.(因此，如果$G$是$m$个 4 阶群的直积，则在$G$中有一个$(4^m, 2\cdot 4^{m-1}-2^{m-1}, 4^{m-1}-2^{m-1})$-差集.)

下面描述已知的几个差集的族. 已知的构造似乎都涉及有限域和/或向量空间. 这些例子中的第一个实质上包含在关于阿达马矩阵的第 18 章中对 Paley 矩阵的讨论中，但值得显式地加以叙述. 参数为

$$(v,k,\lambda) = (4n-1, 2n-1, n-1)$$

的差集通常称为阿达马差集.

**定理 27.5**(Paley, Todd) 设$q=4n-1$是一个素数的幂. 则$\mathbb{F}_q$中的非零平方数的集合$D$是$\mathbb{F}_q$的加法群中的一个$(4n-1, 2n-1, n-1)$-差集.

**证明** 显然$|D|=2n-1$.

因为$D$乘以非零平方数的集合$S$中的元素是不变的，来自$D$的差的多重集$M$也有这个性

质. 显然，$M$ 乘以 $-1$ 也是不变的. 因为 $q\equiv 3 \pmod 4$，$-1\notin S$ 且 $\mathbb{F}_q$ 中的每个非零元素或者属于 $S$ 或者有形式 $-s$，$s\in S$. 总之，$M$ 乘以 $\mathbb{F}_q$ 的所有非零元素是不变的，于是对某个 $\lambda$，$D$ 是一个 $(4n-1,\ 2n-1,\ \lambda)$-差集. 关系 $\lambda(v-1)=k(k-1)$ 迫使 $\lambda=n-1$. ■

375

由定理 27.5，我们在 $\mathbb{Z}_7$，$\mathbb{Z}_{11}$ 和 $\mathbb{Z}_{19}$ 中分别得到差集 $\{1,\ 2,\ 4\}$，$\{1,\ 3,\ 4,\ 5,\ 9\}$ 和 $\{1,\ 4,\ 5,\ 6,\ 7,\ 9,\ 11,\ 16,\ 17\}$. 在这些序列中后面的 $(27,\ 13,\ 6)$-差集将是在 27 阶的基本交换群中，不在 $\mathbb{Z}_{27}$ 中.

**问题 27D** 证明：如果 $q>3$，则 Paley-Todd 差集是正规化的.

Stanton and Sprott(1958)发现了另一族阿达马差集.

**定理 27.6** *如果 $q$ 和 $q+2$ 都是奇素数的幂，$4n-1:=q(q+2)$，则在环 $R:=\mathbb{F}_q\times\mathbb{F}_{q+2}$ 的加法群中存在一个 $(4n-1,\ 2n-1,\ n-1)$-差集.*

**证明** 设 $U:=\{(a,\ b)\in R: a\neq 0,\ b\neq 0\}$ 是 $R$ 的可逆元素的群. 设 $V$ 是 $U$ 的子群，它由在各自的域 $\mathbb{F}_q$ 和 $\mathbb{F}_{q+2}$ 中都是平方数的 $a$，$b$ 或者 $a$ 和 $b$ 都是非平方数的那些对 $(a,\ b)$ 组成. 检查 $V$ 是 $U$ 的指标为 2 的子群，而且 $(-1,\ -1)\notin V$. 置 $T:=\mathbb{F}_q\times\{0\}$. 我们断言 $D:=T\cup V$ 是所要的差集. 我们确实有 $|D|=q+\frac{1}{2}(q-1)(q+1)=2n-1$.

因为 $D$ 在 $V$ 的元素的乘法之下是不变的，来自 $D$ 的差的多重集也有这个性质，以及在 $(-1,\ -1)$ 的乘法之下不变的性质. 因此来自 $D$ 的差的多重集在 $U$ 的所有元素的乘法之下不变. 于是，$U$ 的每个元素作为差出现的次数相同，比如说是 $\lambda_1$. $R$ 中 $x\neq 0$ 的每个元素 $(x,\ 0)$ 作为 $D$ 的一个差出现比如说 $\lambda_2$ 次；$R$ 中 $y\neq 0$ 的每个元素 $(0,\ y)$ 作为 $D$ 的一个差出现比如说 $\lambda_3$ 次. 当然，我们有

$$k(k-1)=(q-1)(q+1)\lambda_1+(q-1)\lambda_2+(q+1)\lambda_3. \tag{27.1}$$

容易计算 $\lambda_2$ 和 $\lambda_3$. 形如 $(x,\ 0)$ 的差，$x\neq 0$（这种形式的元素有 $q-1$ 个），产生于 $T$ 的有 $q(q-1)$ 次，但决不作为 $T$ 的一个元素和 $V$ 的一个元素之间的差，又作为 $V$ 的两个元素的差出现 $(q+1)\cdot\left(\frac{1}{2}(q-1)\right)\left(\frac{1}{2}(q-1)-1\right)$ 次，因此

376

$$(q-1)\lambda_2=q(q-1)+(q+1)\cdot\left(\frac{1}{2}(q-1)\right)\left(\frac{1}{2}(q-1)-1\right),$$

从这个式子我们得出 $\lambda_2=\frac{1}{4}(q+3)(q-1)$. 按照类似的方式（问题 27E），读者会发现 $\lambda_3=\frac{1}{4}(q+3)(q-1)$. 于是 (27.1) 蕴涵 $\lambda_1=\frac{1}{4}(q+3)(q-1)$. ■

**问题 27E** 用定理 27.6 证明中的记号，证明 $\lambda_3=\frac{1}{4}(q+3)(q-1)$.

在 $q$ 和 $q+2$ 都是素数（孪生素数）的情形，定理 27.6 产生循环差集. 这是因为，如果 $s$，$t$ 是互素的整数，$\mathbb{Z}_s\times\mathbb{Z}_t$ 和 $\mathbb{Z}_{st}$ 作为加法群是同构的——而且作为环也是同构的. $\mathbb{Z}_{st}\to\mathbb{Z}_s\times\mathbb{Z}_t$ 的一个同构由 $x \pmod{st}\mapsto(x \pmod s,\ x \pmod t)$ 提供. 在 $\mathbb{Z}_{15}$ 中，我们得到 $(15,\ 7,\ 3)$-差集 $\{0,\ 5,\ 10,\ 1,\ 2,\ 4,\ 8\}$.

**问题 27F** 列出一个循环(35，17，8)-差集的元素.

作为 Singer 定理(即定理 27.7)的一个特殊情形，我们得到阿达马差集的另一个族：参数为

$$v = 2^t - 1, \quad k = 2^{t-1} - 1, \quad \lambda = 2^{t-2} - 1$$

的循环差集.

回忆第 23 章 $PG(n, q)$的点和超平面形成参数为

$$v = \frac{q^{n+1}-1}{q-1}, \quad k = \frac{q^n - 1}{q-1}, \quad \lambda = \frac{q^{n-1}-1}{q-1} \tag{27.2}$$

的一个对称设计.

**定理 27.7** *对任意一个素数的幂 $q$ 和正整数 $n$，在 $v$ 阶循环群中存在一个参数如同(27.2)的差集 $D$，使得由此得到的对称设计同构于 $PG(n, q)$的点和超平面.*

**证明** 根据定理 27.3，我们仅需证明存在 $PG(n, q)$的一个自同构把点排列成长度为 $v$ 的一个单圈，或者等价地，使得这个自同构的幂可迁地作用在射影点上. $PG(n, q)$的点是$\mathbb{F}_q$ 上$(n+1)$维向量空间 $V$ 的 1 维子空间. 从 $V$ 到它自身的任何非奇异的线性变换 $T$ 把子空间变成维数相同的子空间，因此给出 $PG(n, q)$的一个自同构. 377

作为$\mathbb{F}_q$ 上的$(n+1)$维向量空间，我们选择 $V := \mathbb{F}_{q^{n+1}}$ 作为其子域$\mathbb{F}_q$ 上的一个向量空间，设 $\omega$ 为$\mathbb{F}_{q^{n+1}}$的一个本原元并考虑$\mathbb{F}_q$ 上 $V$ 的线性变换 $T: x \mapsto \omega x$. 显然，$T$ 是非奇异的且它的幂在射影点上(甚至在零向量上)是可迁的. ■

在定理 27.7 的证明中构造的差集称为 Singer 差集——见 Singer(1938). 我们给出更具体的讨论和一个例子. 设 $\omega$ 为$\mathbb{F}_{q^{n+1}}$的一个本原元并定义 $v := (q^{n+1}-1)/(q-1)$. $\mathbb{F}_{q^{n+1}}$的循环乘法群$\langle\omega\rangle$有一个阶为 $q-1$ 的唯一的子群，即

$$\langle\omega^v\rangle = \{\omega^0 = 1, \omega^v, \omega^{2v}, \cdots, \omega^{(q-2)v}\}.$$

但子域$\mathbb{F}_q$ 的乘法群的阶为$q-1$，因此我们得出结论：$\mathbb{F}_q = \{0, \omega^0, \omega^v, \omega^{2v}, \cdots, \omega^{(q-2)v}\}$.

现在两个"向量"$\omega^i$ 和 $\omega^j$ 在$\mathbb{F}_{q^{n+1}}$中，$\mathbb{F}_{q^{n+1}}$作为$\mathbb{F}_q$ 上的一个向量空间考虑，$\omega^i$ 和 $\omega^j$ 表示$\mathbb{F}_{q^{n+1}}$的同一个 1 维子空间，当且仅当对某个 $0 \neq \alpha \in \mathbb{F}_q$，$\omega^i = \alpha\omega^j$，即当且仅当 $i \equiv j \pmod{v}$. 因此我们有 1 维子空间(射影点)的集合 $X$ 和模 $v$ 的剩余类的群$\mathbb{Z}_v$ 之间的一个一一对应：

$$0 \leftrightarrow x_0 = \{0, \omega^0, \omega^v, \omega^{2v}, \cdots, \omega^{(q-2)v}\}$$

$$1 \leftrightarrow x_1 = \{0, \omega^1, \omega^{v+1}, \omega^{2v+1}, \cdots, \omega^{(q-2)v+1}\}$$

$$\vdots$$

$$i \leftrightarrow x_i = \{0, \omega^i, \omega^{v+i}, \omega^{2v+i}, \cdots, \omega^{(q-2)v+i}\}$$

$$\vdots$$

$$v-1 \leftrightarrow x_{v-1} = \{0, \omega^{v-1}, \omega^{2v-1}, \omega^{3v-1}, \cdots, \omega^{(q-1)v-1}\}.$$

映射 $x_i \mapsto x_{i+1}$(下标模 $v$)是射影空间的一个自同构. 为得到一个差集，设 $U$ 为$\mathbb{F}_{q^{n+1}}$的任何一个 $n$ 维子空间，再设 $D := \{i \in \mathbb{Z}_v : x_i \in U\}$. 当 $U$ 被取作迹(此迹从$\mathbb{F}_{q^{n+1}}$到$\mathbb{F}_q$)为零的元素的子空间时，得到的差集是正规化的. 378

**例 27.2** 考虑 $n=2$，$q=5$. 我们构造一个(31，6，1)-差集. 多项式 $y^3+y^2+2$(系数在 $\mathbb{F}_5$ 中)的零点 $\omega$ 是 $\mathbb{F}_{5^3}$ 的一个本原元，1，$\omega$，$\omega^2$ 为 $\mathbb{F}_{5^3}$，作为 $\mathbb{F}_5$ 上的一个向量空间，提供了一组基. $\mathbb{F}_{5^3}$ 的 124 个非零元素落入模子群 $\langle\omega^{31}\rangle=\{3，4，2，1\}=\mathbb{F}_5\setminus\{0\}$ 的 31 个陪集中，每个陪集是一个 1 维子空间的非零元. 让我们取 $U:=\mathrm{span}\{1，\omega\}$ 作为一个 2 维子空间. $U$ 上射影点的表示是 1，$\omega$，$\omega+1$，$\omega+2$，$\omega+3$，$\omega+4$，经计算，

$$1=\omega^0$$

$$\omega=\omega^1$$

$$\omega+1=\omega^{29}$$

$$\omega+2=\omega^{99}$$

$$\omega+3=\omega^{80}$$

$$\omega+4=\omega^{84}.$$

得到的 Singer 差集是

$$\mathbb{Z}_{31}\text{ 中的}\{0,1,29,6,18,22\}.$$

**问题 27G** 在 $\mathbb{Z}_{57}$ 中寻找一个(57，8，1)-差集. (有些人可能不想用手算来做这个问题.)

考虑 $n=3$，$q=2$. 这里 $PG(3，2)$ 的点与 $\mathbb{F}_{2^4}$ 中的非零元一一对应，$\mathbb{F}_{2^4}$ 的非零元依次与模 15 的剩余一一对应. 写出这个最小的射影 3-空间中的所有线和平面，使得循环自同构是显然的，这样做可能是有启发意义的.

$y^4+y+1$(系数在 $\mathbb{F}_2$ 中)的零点 $\omega$ 是 $\mathbb{F}_{2^4}$ 的一个本原元且 $\omega^3$，$\omega^2$，$\omega$，1 构成 $\mathbb{F}_4$ 在 $\mathbb{F}_2$ 上的一组基. $\mathbb{F}_{2^4}$ 的任何一个元素可以唯一地写成 $a_3\omega^3+a_2\omega^2+a_1\omega+a_0$，如下简写成 $a_3a_2a_1a_0$. 我们有 $\omega^4+\omega+1=0$ 或 $\omega^4=0011$. 首先我们建立 $\omega$ 的幂的向量表示表.

379

$\mathbb{F}_{2^4}$

| | | |
|---|---|---|
| $\omega^0=0001$ | $\omega^5=0110$ | $\omega^{10}=0111$ |
| $\omega^1=0010$ | $\omega^6=1100$ | $\omega^{11}=1110$ |
| $\omega^2=0100$ | $\omega^7=1011$ | $\omega^{12}=1111$ |
| $\omega^3=1000$ | $\omega^8=0101$ | $\omega^{13}=1101$ |
| $\omega^4=0011$ | $\omega^9=1010$ | $\omega^{14}=1001$ |

$PG(3,2)$

| 线 | | | 平面 |
|---|---|---|---|
| {0,5,10} | {0,1,4} | {0,2,8} | {1,2,4,8,0,5,10} |
| {1,6,11} | {1,2,5} | {1,3,9} | {2,3,5,9,1,6,11} |
| {2,7,12} | {2,3,6} | {2,4,10} | {3,4,6,10,2,7,12} |
| {3,8,13} | {3,4,7} | {3,5,11} | {4,5,7,11,3,8,13} |
| {4,9,14} | {4,5,8} | {4,6,12} | {5,6,8,12,4,9,14} |
| | {5,6,9} | {5,7,13} | {6,7,9,13,5,10,0} |

| | | |
|---|---|---|
| {6,7,10} | {6,8,14} | {7,8,10,14,6,11,1} |
| {7,8,11} | {7,9,0} | {8,9,11,0,7,12,2} |
| {8,9,12} | {8,10,1} | {9,10,12,1,8,13,3} |
| {9,10,13} | {9,11,2} | {10,11,13,2,9,14,4} |
| {10,11,14} | {10,12,3} | {11,12,14,3,10,0,5} |
| {11,12,0} | {11,13,4} | {12,13,0,4,11,1,6} |
| {12,13,1} | {12,14,5} | {13,14,1,5,12,2,7} |
| {13,14,2} | {13,0,6} | {14,0,2,6,13,3,8} |
| {14,0,3} | {14,1,7} | {0,1,3,7,14,4,9} |

注意对 $q=2$，Singer 差集有阿达马参数．我们既从定理 27.5 又从定理 27.7 得到(31，15，7)-差集．这两个差集不等价——甚至不同构．(当两个差集对应的对称设计同构时，这两个差集是同构的．等价的差集一定是同构的，但反之不真．)模 31 的二次剩余的差集 $D$ 有性质

$$D \cap (D+1) \cap (D+3) = \{5,8,10,19\}.$$

380

设计$(\mathbb{Z}_{31}, \{D+g : g\in\mathbb{Z}_{31}\})$与 $PG(4, 2)$的点和超平面不同构，因为平坦面的交仍是平坦面且 $PG(4, 2)$没有正好是四个点的平坦面．

Gordon，Mills，and Welch(1962)已证明 Singer 定理中的构造可以修改成在一些情形得到许多有相同参数但不同构的差集．

**问题 27H** 设 $D$ 是交换群 $G$ 中的一个$(n^2+n+1, n+1, 1)$-差集．证明 $-D$ 是与这个差集相关的射影平面上的一个卵形．

**问题 27I** 设 $G=\{0, a_0, a_1, \cdots, a_q\}$是一个 $q+2$ 阶的任意群，这里 $q$ 是一个素数的幂．设 $V$ 为$\mathbb{F}_q$ 上的一个 2 维向量空间且设 $U_0$，$U_1$，…，$U_q$ 为其 1 维子空间．证明

$$D := \bigcup_{i=0}^{q} \{a_i\} \times U_i$$

是 $G\times V$ 中的一个差集．例如，我们得到一个(45，12，3)-差集．

## 评注

作为循环差集的推广，群差集的思想属于 R. H. Bruck(1955)．

问题 27I 是 McFarland(1973)的一个结果．

定理 27.2 对任意的 2-设计成立，无论它们简单与否．当然，必须对一个任意的关联结构 $\mathbf{S}=(\mathcal{P}, \mathcal{B}, \mathbf{I})$定义自同构．也许最精确的是定义为一个有序对$(\alpha, \beta)$，这里 $\alpha$ 是$\mathcal{P}$的一个置换，$\beta$是$\mathcal{B}$的一个置换，且使得$(x, A)\in\mathbf{I}$ 当且仅当$(\alpha(x), \beta(A))\in I$．在按坐标复合之下，自同构构成一个群．作为自同构群 $\Gamma$ 的第一个坐标出现的置换 $\alpha$ 构成点的置换群 $\Gamma_1$，作为自同构群 $\Gamma$ 的第二个坐标出现的置换$\beta$ 构成区组的置换群 $\Gamma_2$．$\Gamma$ 在点上的轨道是指 $\Gamma_1$ 的轨道，$\Gamma$ 在区组上的轨道是指 $\Gamma_2$ 的轨道．

381

## 参考文献

R. E. Block (1967), On the orbits of collineation groups, *Math Z.* **96**, 33–49.

R. H. Bruck (1955), Difference sets in a finite group, *Trans. Amer. Math. Soc.* **78**, 464–481.

B. Gordon, W. H. Mills, and L. R. Welch (1962), Some new difference sets, *Canad. J. Math.* **14**, 614–625.

R. L. McFarland (1973), A family of difference sets in non-cyclic groups, *J. Combinatorial Theory* (A) **15**, 1–10.

J. Singer (1938), A theorem in finite projective geometry and some applications to number theorey, *Trans. Amer. Math. Soc.* **43**, 377–385.

382

R. G. Stanton and D. A. Sprott (1958), A family of difference sets, *Canad. J. Math.* **10**, 73–77.

# 第28章　差集和群环

群环对差集的研究提供了一个自然且方便的背景．差集的存在性可以被看成等价于群环中一个特定的代数方程的解的存在性．我们将用群环导出 M. Hall, Jr. 的著名的乘子定理，以及关于差集参数的数论准则，这个准则强于 Bruck-Ryser-Chowla 定理．

设 $R$ 为一个(含幺交换)环且 $G$ 是一个有限交换群(写成加法)．群环 $R[G]$ 的元素是所有的形式和

$$A=\sum_{g\in G}a_g x^g,$$

其中对每个 $g\in G$，$a_g\in R$.(这里符号 $x$ 仅是占位符.)重要的是对 $G$ 的每个元素 $g$ 我们有 $R$ 中的一个元素 $a_g$，即群环的元素与映射 $G\to R$ 是一一对应的．

我们以明显的方式定义加法和标量乘法：

$$\sum_{g\in G}a_g x^g+\sum_{g\in G}b_g x^g:=\sum_{g\in G}(a_g+b_g)x^g,$$

$$c\sum_{g\in G}a_g x^g:=\sum_{g\in G}(ca_g)x^g.$$

$R[G]$中的乘法由

$$\sum_{g\in G}a_g x^g\sum_{g\in G}b_g x^g:=\sum_{g\in G}\Big(\sum_{h+h'=g}a_h b_{h'}\Big)x^g$$

定义．

383

根据这些定义，$R[G]$是一个交换、结合的 $R$-代数．我们选择的符号适合交换群且强调与多项式的类似．注意当 $G$ 是模 $v$ 的剩余的加法群时，群环 $R[\mathbb{Z}_v]$由所有的和 $\sum_{i=0}^{v-1}r_i x^i$（指数模 $v$）构成且同构于多项式环 $R[x]$的分式环 $R[x]/(x^v-1)$．一般地，我们在方便时甚至把任意群环 $R[G]$的元素取作 $A(x)$，$B(x)$，$\cdots$．元素 $x^0\in R[G]$是 $R[G]$中乘法的单位元并用 1 表示 $x^0$．

我们所关心的几乎集中在整数的群环$\mathbb{Z}[G]$上．对一个子集 $A\subseteq G$，由

$$A(x)=\sum_{g\in A}x^g$$

定义 $A(x)\in\mathbb{Z}[G]$．特别地，$G(x)=\sum_{g\in G}x^g$．对 $A$，$B\subseteq G$，

$$A(x)B(x)=\sum_{g\in G}c_g x^g,$$

这里 $c_g$ 是 $g$ 出现在 $A$ 和 $B$ 的元素之和的多重集

$$(h+h':h\in A,h'\in B)$$

中的次数．

对 $A(x)=\sum_{g\in G}a_g x^g\in\mathbb{Z}[G]$，我们写出

$$A(x^{-1}):=\sum_{g\in G}a_g x^{-g}.$$

于是对 $v$ 阶群 $G$ 的一个 $k$-子集 $D$，$D$ 是 $G$ 中的一个$(v,k,\lambda)$-差集当且仅当等式

$$D(x)D(x^{-1}) = n + \lambda G(x)$$

在群环$\mathbb{Z}[G]$中成立，这里 $n := k-\lambda$.

从$\mathbb{Z}[G]$到$\mathbb{Z}$的一个重要的同态由

$$A(x) \mapsto A(1) := \sum_{g\in G} a_g \in \mathbb{Z}$$

384 给出.

**命题 28.1** 设 $v$，$k$，$\lambda$ 是使得

$$\lambda(v-1) = k(k-1)$$

的正整数，又设 $G$ 是一个 $v$ 阶的交换群. 在 $G$ 中存在一个$(v, k, \lambda)$-差集等价于存在一个元素 $A(x)\in\mathbb{Z}[G]$满足方程

$$A(x)A(x^{-1}) = n + \lambda G(x), \tag{28.1}$$

这里 $n := k-\lambda$.

**证明** 我们已经指出对 $G$ 的一个子集 $D$，$D(x)$满足(28.1)当且仅当 $D$ 是一个$(v, k, \lambda)$-差集. 剩下的要证明如果(28.1)存在一个解 $A(x)$，则我们能找到一个解 $B(x) = \sum_{g\in G} b_g x^g$，这里系数 $b_g$ 是 0 或 1.

假定 $A(x)$满足(28.1)并应用$\mathbb{Z}[G]\to\mathbb{Z}$的同态“$x \mapsto 1$”. 我们发现

$$(A(1))^2 = n + \lambda v = k^2,$$

因此 $A(1)=k$ 或 $-k$. 现在，如果 $A(x)$满足(28.1)，则 $B(x)=-A(x)$亦然，因此可以假设 $A(1)=\sum a_g = k$.

在 $A(x)A(x^{-1})$中，$1=x^0$ 的系数是 $k=\sum_{g\in G} a_g^2$. 于是 $\sum_{g\in G} a_g(a_g-1)=0$. 但 $a(a-1)$是严格正的，除非整数 $a$ 等于 0 或 1. ■

对任意整数 $t$，$g \mapsto tg$ 是群 $G$ 到自身的一个同态并导出环同态$\mathbb{Z}[G]\to\mathbb{Z}[G]$，即

$$A(x) = \sum_{g\in G} a_g x^g \mapsto A(x^t) := \sum_{g\in G} a_g x^{tg}.$$

对 $A$，$B\in\mathbb{Z}[G]$且 $n\in\mathbb{Z}$，当对某一 $C\in\mathbb{Z}[G]$，$A-B=nC$ 时，我们说 $A\equiv B \pmod n$. 下面给出一个经常要用的易证的引理.

**引理 28.2** 设 $p$ 是一个素数且 $A\in\mathbb{Z}[G]$，则

385
$$(A(x))^p \equiv A(x^p) \pmod p.$$

**证明** 我们对 $A(x)$的非零系数的个数进行归纳. 当 $A(x)=0$ 时引理成立. 如果$A(x)=cx^g+B(x)$，这里 $B^p(x)\equiv B(x^p) \pmod p$，则

$$\begin{aligned} A^p(x) &= (cx^g + B(x))^p \equiv (cx^g)^p + B^p(x) \\ &= c^p x^{pg} + B^p(x) \equiv cx^{pg} + B(x^p) = A(x^p), \end{aligned}$$

这里同余是模 $p$ 的. ■

设 $G$ 为一个交换群且 $D$ 为 $G$ 中的差集，$G$ 的自同构 $\alpha$ 称为 $D$ 的一个乘子，当且仅当差集 $\alpha(D)$实际上是 $D$ 的一个平移，即当且仅当对某一 $g\in G$，$\alpha(D)=D+g$. 例如，$\mathbb{Z}_{13}$的自同构

$x \mapsto 3x$ 是 $(13, 4, 1)$-差集 $\{0, 2, 3, 7\}$ 的一个乘子，因为 $\{0, 6, 9, 8\} = \{0, 2, 3, 7\} + 6$.

如果 $t$ 是一个与 $G$ 的阶互素的整数，则 $x \mapsto tx$ 是 $G$ 的一个自同构，因为映射 $x \mapsto t_1 x$ 和 $x \mapsto t_2 x$ 重合当且仅当 $t_1 \equiv t_2 \pmod{v^*}$，这里 $v^*$ 是 $G$ 的指数，即 $G$ 的元素的阶的最小公倍数. 如果 $x \mapsto tx$ 是 $G$ 中差集 $D$ 的一个乘子，我们说 $t$ 是 $D$ 的数值乘子或霍尔(Hall)乘子. 首先令人惊奇的是许多差集(例如人所共知的循环差集)必定有一个非平凡的数值乘子.

**问题 28A** 设 $q = p^t$，$p$ 为素数. 证明 $p$ 是上一章中描述的 Singer 差集的一个乘子.

注意 $G$ 的自同构 $\alpha$ 是 $G$ 中的差集 $D$ 的一个乘子，当且仅当在群环 $\mathbb{Z}[G]$ 中对某一 $g \in G$，$D(x^\alpha) = x^g \cdot D(x)$.

**定理 28.3**(乘子定理，第一种叙述) 设 $D$ 是 $v$ 阶交换群 $G$ 中的一个 $(v, k, \lambda)$-差集. 设 $p$ 为一个素数，$p \mid n$，$(p, v) = 1$，$p > \lambda$. 则 $p$ 是 $D$ 的一个数值乘子.

把该定理的部分证明概括为下面的引理.

**引理 28.4** 设 $\alpha$ 为 $G$ 的一个自同构，又设 $D$ 为 $G$ 中的一个 $(v, k, \lambda)$-差集. 考虑

$$S(x) := D(x^\alpha) D(x^{-1}) - \lambda G(x).$$

386

则 $\alpha$ 是 $D$ 的一个乘子当且仅当 $S(x)$ 有非负的系数.

**证明** 首先我们说，如果 $\alpha$ 是一个乘子，则对某个 $g \in G$ 有 $D(x^\alpha) = x^g \cdot D(x)$，且

$$D(x^\alpha) D(x^{-1}) = x^g \cdot D(x) D(x^{-1}) = x^g (n + \lambda G(x)) = n x^g + \lambda G(x).$$

因此在这一情形，如上面所定义的，对某个 $g \in G$，$S(x)$ 等于 $n x^g$. 特别地，它有非负的系数. 注意，反之，如果 $D(x^\alpha) D(x^{-1}) = n x^g + \lambda G(x)$，我们可以乘以 $D(x)$ 得到

$$D(x^\alpha) \cdot (n + \lambda G(x)) = n x^g \cdot D(x) + \lambda D(x) G(x),$$

$$n D(x^\alpha) + \lambda k G(x) = n x^g \cdot D(x) + \lambda k G(x).$$

因此 $D(x^\alpha) = x^g \cdot D(x)$ 且 $\alpha$ 是一个乘子.

现在“$x \mapsto x^\alpha$”是 $\mathbb{Z}[G]$ 的一个自同构，于是 $D(x^\alpha) D(x^{-\alpha}) = n + \lambda G(x)$，即 $\alpha(D)$ 也是一个差集，且

$$\begin{aligned} S(x) S(x^{-1}) &= \{D(x^\alpha) D(x^{-1}) - \lambda G(x)\}\{D(x^{-\alpha}) D(x) - \lambda G(x)\} \\ &= \{n + \lambda G(x)\}^2 - 2\lambda k^2 G(x) + \lambda^2 v G(x) \\ &= n^2 + 2\lambda(n + \lambda v - k^2) G(x) = n^2. \end{aligned}$$

假设 $S(x) = \sum_{g \in G} s_g x^g$ 有非负系数 $s_g$. 如果对 $g, h \in G$，$s_g > 0$ 且 $s_h > 0$，则 $x^{g-h}$ 的系数在 $S(x) S(x^{-1}) = n^2$ 中至少是 $s_g s_h$，即严格正的，因此 $x^{g-h} = x^0$，即 $g = h$. 于是 $S(x)$ 仅有一个正的系数，比如说 $S(x) = s_g x^g$. 方程 $S(x) S(x^{-1}) = n^2$ 迫使 $s_g = n$，我们已经证明 $S(x) = n x^g$. 如上面注意到的，可以得出 $\alpha$ 是一个乘子. ■

**定理 28.3 的证明** 设 $S(x) := D(x^p) D(x^{-1}) - \lambda G(x)$. 由引理 28.4，证明 $S(x)$ 有非负系数就够了. 由引理 28.2，因为 $p$ 整除 $n$ 且 $\lambda k^{p-1} \equiv \lambda^p \equiv \lambda \pmod{p}$，

$$\begin{aligned} D(x^p) D(x^{-1}) &\equiv D^p(x) D(x^{-1}) \equiv D^{p-1}(x) D(x) D(x^{-1}) \\ &\equiv D^{p-1}(x) \cdot (n + \lambda G(x)) \equiv n D^{p-1}(x) + \lambda k^{p-1} G(x) \end{aligned}$$

[387]

$$\equiv \lambda G(x)(\text{mod } p),$$

因此 $D(x^p)(x^{-1})$的系数显然非负，且模 $p$ 都与$\lambda$ 同余．因为 $p>\lambda$，$D(x^p)D(x^{-1})$的系数大于或等于$\lambda$，即 $S(x)$的系数非负．■

**问题 28B**　在$\mathbb{Z}[\mathbb{Z}_7]$中寻找一个元素 $S(x)$，它有性质 $S(x)S(x^{-1})=4$，但 $S(x)\neq\pm 2x^{\kappa}$.

注意在我们的证明中假设 $p>\lambda$ 是基本的．然而，在每个已知的差集中，$n$ 的每个素因子(不整除 $v$)是一个乘子．那么，假设 $p>\lambda$ 可能不是必需的，但现在这个问题获得了经典的未解决的问题之誉．原始的乘子定理有几个推广，如果我们能消去条件 $p>\lambda$，这些推广就都是平凡的，我们首先给出当前叙述的定理的应用，然后讨论一个推广．

**推论**　对$\lambda=1$，$n$ 的每个素因子，因此 $n$ 的每个因子是每个$(n^2+n+1,\ n+1,\ 1)$-差集的乘子．

**例 28.1**　我们断言没有 $n\equiv 0(\text{mod } 6)$的$(n^2+n+1,\ n+1,\ 1)$-差集．假设 $D$ 是这样的一个差集，不失一般性，假设 $D$ 是正规化的，因此它被所有的乘子固定．2 和 3 都是乘子，则对 $x\in D$，$2x$ 和 $3x$ 也在 $D$ 中．则差 $x$ 出现两次，一次作为 $2x-x$，另一次作为 $3x-2x$；只要 $3x\neq 2x$，即 $x\neq 0$，这些就是不同的．这与$\lambda=1$ 矛盾．

**问题 28C**　$n$ 能被 10，14，15，21，22，26，34，35 中的任何一个整除，证明不存在$(n^2+n+1,\ n+1,\ 1)$-差集．

用乘子定理和其他方法，可以证明对 $n\leqslant 3600$ 不存在平面差集，除非 $n$ 是一个素数的幂．但在 $n$ 一定是素数的幂时，猜想仍未解决．

**例 28.2**　在$\mathbb{Z}_{21}$中考虑一个正规化的(21，5，1)-差集 $D$．由乘子定理，2 是一个乘子，因此 $2D=D$．于是 $D$ 一定是$\mathbb{Z}_{21}$上 $x\mapsto 2x$ 的圈的并．这些圈是

[388]

$$\{0\},\quad \{1,2,4,8,16,11\},\quad \{3,6,12\},\quad \{5,10,20,19,17,13\},\quad \{7,14\},\quad \{9,18,15\}.$$

但 $D$ 有 5 个元素，因此，如果有这样一个差集，$D$ 一定是{7，14，3，6，12}或{7，14，9，8，15}．结果是两者都是差集．一个差集由另一个差集的相反数组成，因此具有这些参数的 42 个差集都是等价的．

**问题 28D**　找出参数为(7，3，1)，(11，5，2)，(13，4，1)，(19，9，4)，(31，10，3)和(37，9，2)的所有正规化差集．(注意：这些参数三元组之一不存在差集．)

下面给出关于群环的两个更为容易的引理．

**引理 28.5**　设 $G$ 是一个 $v$ 阶的交换群且 $p$ 为一个素数，$p\nmid v$．设 $A\in\mathbb{Z}[G]$且对某一正整数 $m$，$A^m\equiv 0(\text{mod } p)$．则 $A\equiv 0(\text{mod } p)$．

**证明**　选择 $p$ 的一个幂$q=p^e$ 使得$q\geqslant m$ 且$q\equiv 1(\text{mod } v)$．那么一定有 $A^q(x)\equiv 0(\text{mod } p)$．但由引理 28.2，$A^q(x)\equiv A(x^q)(\text{mod } p)$，因此 $A(x^q)\equiv 0(\text{mod } p)$．因为 $q\equiv 1(\text{mod } v)$，对某个 $g\in G$，$qg=g$，且 $A(x)=A(x^q)$．■

注意，在$\mathbb{Z}[G]$中 $x^g\cdot G(x)=G(x)$．由此得出

$$A(x)G(x) = A(1)G(x).$$

对 $n\in\mathbb{Z}$ 和 $A$，$B\in\mathbb{Z}[G]$，当 $A-B$ 是由 $n$ 和 $G=G(x)$生成的$\mathbb{Z}[G]$中理想的一个元素时，或者等价地，对某一 $C\in\mathbb{Z}[G]$，

$$A - B = nC + mG$$

时，我们说$A \equiv B(\bmod\ n,\ G)$.

**引理 28.6** 设$G$为一个$v$阶的交换群且$p$为一个素数，$p \nmid v$. 如果$A \in \mathbb{Z}[G]$且对某个正整数$m$，

$$A^m \equiv 0(\bmod\ p, G),$$

则$A \equiv 0(\bmod\ p,\ G)$.

**证明** 选择$q = p^e$满足$q \equiv 1(\bmod\ v)$且$q \geq m$. 则$A^q(x) \equiv 0(\bmod\ p,\ G)$且$A^q(x) \equiv A(x^q) = A(x)(\bmod\ p)$. ■ 389

**定理 28.7**（乘子定理，第二种叙述） 设$D$是指数为$v^*$的交换群$G$中的一个$(v,\ k,\ \lambda)$-差集. 设$t$为整数，$(t,\ v)=1$，又假设可以找到$n := k-\lambda$的一个因子$m$使得$m > \lambda$，且对$m$的每个素因子$p$，存在一个整数$f$，对$f$有$p^f \equiv t(\bmod\ v^*)$，则$t$是$D$的一个数值乘子.

**证明** 证明要利用引理 28.2、引理 28.4、引理 28.5 和如下的观察：

设$D$为$G$中的一个$(v,\ k,\ \lambda)$-差集，$\alpha$为$G$的一个自同构，又置$S(x) := D(x^\alpha)D(x^{-1}) - \lambda G(x)$. 假设$\alpha$的阶为$e$，所以$\alpha^e =$单位元. 那么，我们断言在群环$\mathbb{Z}[G]$中，

$$S(x)S(x^\alpha)S(x^{\alpha^2})\cdots S(x^{\alpha^{e-1}}) = n^e.$$

为了明白这一点，注意对任意的一个整数$i$，我们有

$$D(x^{\alpha^i})D(x^{-\alpha^i}) = n + \lambda G(x) \equiv n(\bmod\ G)$$

以及

$$\begin{aligned} S(x^{\alpha^i}) &= D(x^{\alpha^{i+1}})D(x^{-\alpha^i}) - \lambda G(x) \\ &\equiv D(x^{\alpha^{i+1}})D(x^{-\alpha^i})(\bmod\ G). \end{aligned}$$

则

$$\begin{aligned} &S(x)S(x^\alpha)s(x^{\alpha^2})\cdots S(x^{\alpha^{e-1}}) \\ \equiv&\{D(x^\alpha)D(x^{-1})\}\{D(x^{\alpha^2})D(x^{-\alpha})\}\cdots\{D(x)D(x^{-\alpha^{e-1}})\} \\ \equiv&\{D(x)D(x^{-1})\}\{D(x^\alpha)D(x^{-\alpha})\}\cdots\{D(x^{\alpha^{e-1}})D(x^{-\alpha^{e-1}})\} \\ \equiv&n^e(\bmod\ G). \end{aligned}$$

因此对某个整数$\ell$，$S(x)S(x^\alpha)\cdots S(x^{\alpha^{e-1}}) = n^e + \ell G(x)$. 但$S(1) = (D(1))^2 - \lambda G(1) = k^2 - \lambda v = n$，因此应用同态$x \mapsto 1$，得到$n^e = n^e + \ell v$，从而$\ell = 0$.

为继续证明，设$S(x) := D(x^t)D(x^{-1}) - \lambda G(x)$. 由引理 28.4，为证明$t$是一个乘子，证明$S(x)$的系数非负就够了. $S(x)$的每个系数的取值至少是$-\lambda$，因为$m > \lambda$，系数的非负性可以从$S(x) \equiv 0(\bmod\ m)$得出，如果我们能建立这个关系. 为此，只要证明$S(x) \equiv 0(\bmod\ p^i)$即可，只要$p$是素数且$p^i$整除$m$. 我们证明如下. 390

设$e$是$t$模$v^*$的阶，因此$t^e \equiv 1(\bmod\ v^*)$. 如上所证，

$$S(x)S(x^t)S(x^{t^2})\cdots S(x^{t^{e-1}}) = n^e.$$

设$p$为$m$的一个素因子并设$f$使得$p^f \equiv t(\bmod\ v^*)$，则

$$S(x)S(x^{p^f})S(x^{p^{2f}})\cdots S(x^{p^{f(e-1)}}) = n^e.$$

设$p^i$为整除$n$的$p$的最高次幂，$p^j$为整除$S(x)$（的所有系数）的$p$的最高次幂，于是

$S(x)=p^j T(x)$，这里 $T(x)\not\equiv 0 \pmod p$. 则

$$p^j T(x) p^j T(x^{p^f}) \cdots p^j T(x^{p^{f(e-1)}}) = n^e,$$

由此得出 $p^j$ 整除 $n$（因此 $j\leqslant i$）且

$$T(x)T(x^{p^f})\cdots T(x^{p^{f(e-1)}}) = \left(\frac{n}{p^j}\right)^e.$$

假设 $j<i$，所以 $\left(\frac{n}{p^j}\right)^e$ 能被 $p$ 整除. 则

$$\begin{aligned} 0 &\equiv T(x)T(x^{p^f})\cdots T(x^{p^{f(e-1)}}) \\ &\equiv T(x)T^{p^f}(x)\cdots T(x)T^{p^{f(e-1)}}(x) \\ &\equiv (T(x))^{1+p^f+\cdots+p^{f(e-1)}} \pmod p. \end{aligned}$$

但由引理 28.5，$T(x)\not\equiv 0 \pmod p$，与 $j$ 的选择矛盾. 因此 $i=j$. ■

**推论** *如果 $n=p^e$，$p$ 是素数，$(p, v)=1$，则 $p$ 是每个 $(v, k, \lambda)$-差集的一个数值乘子.*

**证明** 差集 $D$ 与它的补 $G\setminus D$ 有相同的乘子. 因此可以设 $k<\frac{1}{2}v$，于是 $n>\lambda$. 在定理

[391] 28.7 中，取 $m=n$，$t=p$. ■

**例 28.3** 考虑一个假想的(25，9，3)-差集. 在上面的定理中取 $t=2$ 且 $m=6$. 因为 $3^3\equiv 2 \pmod{25}$，我们可能得出 2 是一个乘子的结论.

**问题 28E** 找出参数为(15，7，3)，(25，9，3)，(39，19，9)，(43，15，5)和(61，16，4)的所有正规化差集. 对每个参数集，确定这些正规化差集是否等价.（注意：对绝大多数参数集，差集不存在.）

**问题 28F** 设 $D$ 为一个非平凡的 $(v, k, \lambda)$-差集. 证明：如果 $-1$ 是 $D$ 的一个乘子，则 $v$ 是偶数.

**问题 28G** 在 $\mathbb{Z}_6\times\mathbb{Z}_6$ 中寻找一个 $-1$ 为其乘子的(36，15，6)-差集.

* * *

设 $D$ 是偶阶 $v$ 的交换群 $G$ 的一个 $(v, k, \lambda)$-差集. 由定理 19.11(i)，我们知道 $n$ 是一个平方数. 但在差集的情形，我们可以说 $n$ 是*谁的平方*！设 $A$ 为群 $G$ 的指标为 2 的任意一个子群. 比如说 $D$ 包含 $A$ 的 $a$ 个元素和 $B:=G\setminus A$ 的 $b$ 个元素. 因为 $B$ 中的每个元素作为来自 $D$ 的差出现 $\lambda$ 次，而只作为 $A$ 中一个元素和 $B$ 中一个元素落入 $B$ 中的差，所以 $2ab=\frac{1}{2}\lambda v$. 由这个式子和 $a+b=k$，我们得到 $(a-b)^2=n$.

现在假设 $v$ 能被 3 整除，设 $A$ 是 $G$ 的指标为 3 的一个子群，设 $B$ 和 $C$ 是 $A$ 在 $G$ 中的陪集. 比如说 $D$ 包含 $A$ 中的 $a$ 个元素，$B$ 中的 $b$ 个元素，$C$ 中的 $c$ 个元素. 来自 $D$ 的差落入 $B$ 的数目，比如说是 $ba+cb+ac$，另一方面这个数目一定是 $\frac{1}{3}\lambda v$. 由这个关系和 $a+b+c=k$，我们可以验证 $4n=(b+c-2a)^2+3(b-c)^2$. 每一个整数能写成一个平方数与三倍的另一个平方数之和不真，因此这个条件排除了某些差集的存在. 例如，因为 $4n=40$ 不能写成一个平方数和三倍的另一个平方数之和，所以不存在(39，19，9)-差集，尽管对这些参数存在对称设计.

我们通过考虑群环的同态推广上面关于差集的参数的必要条件. 如果 $\alpha$ 是一个同态 $G\to H$，则 $\alpha$ 诱导出一个环同态 $\mathbb{Z}[G]\to\mathbb{Z}[H]$： [392]

$$A(x)=\sum a_g x^g \mapsto A(x^\alpha):=\sum a_g x^{\alpha(g)}\in\mathbb{Z}[H].$$

**定理 28.8** 设 $D$ 是交换群 $G$ 中的一个 $(v,k,\lambda)$-差集. 设 $u>1$ 是 $v$ 的一个因子. 如果 $p$ 是 $n$ 的一个素因子且对某个整数 $f$，

$$p^f\equiv -1\pmod{u},$$

则 $p$ 不整除 $n$ 的平方因子之外的部分.

**证明** 我们证明更强的结论. 比如说，设 $\alpha: G\to H$ 是到阶为 $u$ 且指数为 $u^*$ 的群 $H$ 的同态. 假设 $p$ 是素数且对某个 $f$，$p^f\equiv -1(\bmod u^*)$. 我们证明 $n$ 恰能被 $p$ 的偶次幂 $p^{2j}$ 整除且对这个 $j$，在 $\mathbb{Z}[H]$ 中

$$D(x^\alpha)\equiv 0\pmod{p^j,H}.$$

换言之，$D(x^\alpha)$ 的所有系数彼此模 $p^j$ 同余，这些系数是 $D$ 中属于 $\alpha$ 的核的不同陪集的元素数.

设 $p^i$ 是整除 $n$ 的 $p$ 的最大幂. 假设 $p^f\equiv -1(\bmod u^*)$ 意味着在 $\mathbb{Z}[H]$ 中 $D(x^{-\alpha})=D(x^{p^f\alpha})$（这里我们将做运算），因此有

$$\begin{aligned}D(x^\alpha)D(x^{p^f\alpha})&=D(x^\alpha)D(x^{-\alpha})\\&=n+\lambda\frac{v}{u}H(x)\equiv 0(\bmod p^i,H).\end{aligned}\tag{28.2}$$

设 $p^j$ 是 $p$ 的最大幂使得 $D(x^\alpha)\equiv 0(\bmod p^j,H)$；比如说 $D(x^\alpha)\equiv p^jA(x)(\bmod H)$. 读者可以验证(28.2)蕴涵 $2j\leqslant i$；如果 $2j<i$，则 $A(x)A(x^{p^f})\equiv 0(\bmod p,H)$. 那么引理 28.2 和引理 28.6 依次蕴涵 $A(x)^{1+p^f}\equiv 0(\bmod p,H)$ 和 $A(x)\equiv 0(\bmod p,H)$. 这与 $j$ 的选择矛盾，所以 $2j=i$. ■

定理 28.8 的结论是：如果 $v$ 能被 3 整除，则 $n$ 的平方因子之外的所有素因子模 3 同余于 0 或 1；如果 $v$ 能被 5 整除，则 $n$ 的平方因子之外的所有素因子模 5 同余于 0 或 1；如果 $v$ 能被 7 整除，则 $n$ 的平方因子之外的素因子模 7 同余于 0，1，2 或 4. [393]

**例 28.4** 我们给出在定理 28.8 的证明中所给的较强断言的一个应用. 考虑 $G$ 中一个假设的(154，18，2)-差集. 设 $\alpha: G\to H$ 是到一个阶为 $u:=11$ 的群 $H$ 上的同态. 取 $p:=2$. 因为 $2^5\equiv -1(\bmod 11)$，我们得出 $D(x^\alpha)\equiv 0(\bmod 4,H)$. 这意味着 $D(x^\alpha)$ 的 11 个系数模 4 都同余于某个整数 $h$；因为 11 个系数的和是 18，所以 $h$ 等于 2. 那么系数的和至少是 22，这个矛盾证明这样的差集不存在.

**问题 28H** 设 $D$ 是交换群 $G$ 中的一个 $(q^4+q+1,\ q^2+1,\ 1)$-差集. 设 $\alpha: G\to H$ 是到一个阶为 $u:=q^2-q+1$ 的群 $H$ 上的同态. 证明 $\alpha$ 的核的任意一个陪集是阶为 $q^2$ 的射影平面的一个白尔子平面的点集，射影平面来自 $D$. 例如，4 阶射影平面的 21 个点被划分成三个费诺构形.

**问题 28I** 设 $D$ 是交换群 $G$ 中的一个 $(q^3+q^2+q+1,\ q^2+q+1,\ q+1)$-差集. 设 $\alpha: G\to H$ 是到一个阶为 $u:=q+1$ 的群 $H$ 上的同态. 证明 $D$ 的平移交 $\alpha$ 的核于 $q+1$ 个点或单独一个点. 进一步证明，如果来自 $D$ 的对称设计由 $PG_3(q)$ 的点和平面组成，则陪集是卵形面（见例 26.5）.

## 评注

著名的乘子定理首先由 Hall(1947)对循环平面差集加以证明. 它被 Hall and Ryser(1951)扩展到 $\lambda>1$, 此后在许多方面被推广——例如, 见 Mann(1965)、Baumert(1971)以及 Lander(1983). 代数数论和交换群的性质在这些结果的证明中常常起作用, 但我们这里选择仅用群环给出定理 28.7 和定理 28.8 的证明.

霍尔(Marshall Hall, 1910－1990)在群论、编码理论及组合设计中做了重要的工作. 他对许多数学家有巨大影响, 包括本书的两位作者.

394

定理 28.8 属于 K. Yamamoto(1963).

## 参考文献


L. D. Baumert (1971), *Cyclic Difference Sets*, Lecture Notes in Math. **182**, Springer-Verlag.

M. Hall (1947), Cyclic projective planes, *Duke J. Math.* **14**, 1079–1090.

M. Hall and H. J. Ryser (1951), Cyclic incidence matrices, *Canad. J. Math.* **3**, 495–502.

E. S. Lander (1983), *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lecture Note Series **74**, Cambridge University Press.

H. B. Mann (1965), *Addition Theorems*, Wiley.

K. Yamamoto (1963), Decomposition fields of difference sets, *Pacific J. Math.* **13**, 337–352.


395

# 第29章 码和对称设计

本章将详述第 20 章引入的一些内容，在那一章我们已看到阶 $n\equiv 2 \pmod 4$ 的射影平面的关联矩阵的行生成一个二元码，在扩展时它是自对偶的. H. A. Wilbrink(1985)和其他一些人观察到这个结果可用来证明对 $n>2$ 且 $n\equiv 2 \pmod 4$ 的 $n$ 值，不存在平面差集；见定理 29.7.

也可以考虑其他素数域$\mathbb{F}_p$ 上的关联矩阵的行生成的码. 由与定理 20.6 的证明本质上相同的证明，我们有如下定理.

**定理 29.1** *如果 $p$ 整除 $n:=k-\lambda$，则一个对称$(v, k, \lambda)$-设计的关联矩阵 $N$ 的行的$\mathbb{F}_p$-生成 $C$ 在$\mathbb{F}_p$ 上的维数至多为$(v+1)/2$. 如果$(p, k)=1$ 且 $p^2$ 不整除 $n$，则这个 $p$ 元码的维数恰好为$(v+1)/2$.*

**问题 29A** 证明定理 29.1.

一般地，扩充码 $C$ 以得到一个长度为 $v+1$ 的关于$\mathbb{F}_p^v$上的标准点积自正交的码是不可能的. 下面对奇素数 $p$ 考虑其他"标量积".

对域$\mathbb{F}$ 上的一个非奇异的 $m\times m$ 矩阵 $B$，及 $\boldsymbol{x}$，$\boldsymbol{y}\in\mathbb{F}^m$，我们可以联系标量积(或双线性型)

$$\langle \boldsymbol{x},\boldsymbol{y}\rangle := \boldsymbol{x}B\boldsymbol{y}^\top.$$

对$\mathbb{F}^m$的一个子空间 $C$，设

$$C^B := \{\boldsymbol{x} : \langle \boldsymbol{x},\boldsymbol{y}\rangle = 0, \text{对所有 } \boldsymbol{y}\in C\}.$$

396

则 $C$ 和 $C^B$ 有互补的维数且$(C^B)^B=C$. 当 $C\subseteq C^B$ 时，我们说 $C$ 是完全迷向的，对于这个自正交的推广而言，这是一个合适术语. 这一术语应用于如下的维特(Witt)定理，这里包括一个证明，这个定理本质上是定理 26.6 部分内容的另一种描述.

**定理 29.2** *在有奇特征的域$\mathbb{F}$ 上给定一个对称的非奇异矩阵 $B$，在$\mathbb{F}^m$ 中存在一个维数为 $m/2$ 的完全迷向的子空间，当且仅当$(-1)^{m/2}\det(B)$在$\mathbb{F}$ 中是一个平方数.*

**证明** 一个维数为 $m/2$ 的完全迷向的子空间，在作为 $PG(m-1, 2)$中射影点的一个集合考虑时，是射影维数为$(m/2)-1$ 的一个平坦面，该平坦面完全包含在由非退化的二次型

$$f(\boldsymbol{x}) = \boldsymbol{x}B\boldsymbol{x}^\top$$

定义的二次曲面 $Q$ 中. 由定理 26.6，这样的子空间存在，当且仅当 $Q$ 是双曲的. 剩下的只要验证 $Q$ 是双曲的当且仅当$(-1)^{m/2}\det(B)$在$\mathbb{F}$ 中是一个平方数.

如果 $f_1$ 是射影等价于 $f$ 的型，则 $f_1(\boldsymbol{x})=\boldsymbol{x}B_1\boldsymbol{x}^\top$，这里 $B_1=UBU^\top$，$U$ 为某个非奇异矩阵. 当然，$(-1)^{m/2}\det(B)$是一个平方数当且仅当$(-1)^{m/2}\det(B_1)$是一个平方数.

如果 $Q$ 是双曲的，则 $f$ 等价于 $f_1=x_1x_2+\cdots+x_{m-1}x_m$ 且 $B_1$ 是 $m/2$ 个矩阵

$$W = \frac{1}{2}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

在对角线上的分块对角阵. 因此，$(-1)^{m/2}\det(B_1)=1/2^m$ 是一个平方数.

如果 $Q$ 是椭圆的，则 $f$ 等价于 $f_1=x_1x_2+\cdots+x_{m-3}x_{m-2}+p(x_{m-1}, x_m)$，这里 $p(x, y)=$

$ax^2+2bxy+cy^2$ 是$\mathbb{F}$上的一个不可约二次型，且 $B_1$ 是$(m/2)-1$ 个矩阵 $W$ 和一个矩阵

$$\begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

在对角线上的分块对角阵，因此$(-1)^{m/2}\det(B_1)=(b^2-ac)/2^{m-2}$，因为 $p$ 是不可约的，这个结果在$\mathbb{F}$中不是一个平方数. ■

397

对维数等于其长度一半的一个完全迷向的子空间，保留术语自对偶是方便的. E. S. Lander(1983)已证明如何联系长度为 $n+1$ 的 $p$ 元码的一个族和一个纯量积到一个对称设计，使得当 $n$ 恰能被 $p$ 的一个奇次幂整除时，码中有一个是自对偶的. 此时定理 29.2 给出有关对称设计的参数的一个条件. 得出这些条件是 Bruck-Ryser-Chowla 定理(即定理 19.11)的结论. 在某种意义上，这些自对偶码提供了部分 BRC 定理的"组合解释". 在每种情形，这些码带有设计的信息且在对称设计理论中有进一步的应用——见 Lander(1983).

**定理 29.3**　*假定存在一个对称的$(v, k, \lambda)$-设计，这里 $n$ 恰能被一个奇素数 $p$ 的奇次幂整除. 写成 $n=p^f n_0$($f$ 为奇数)且 $\lambda=p^b\lambda_0$，$(n_0, p)=(\lambda_0, p)=1$. 则相对于与*

$$B=\begin{cases}\operatorname{diag}(1,1,\cdots,1,-\lambda_0) & \text{如果 } b \text{ 为偶数,}\\ \operatorname{diag}(1,1,\cdots,1,n_0\lambda_0) & \text{如果 } b \text{ 为奇数}\end{cases}$$

*对应的标量积，存在一个长度为 $v+1$ 的自对偶 $p$ 元码. 因此，由定理 29.2，*

$$\begin{cases}-(-1)^{(v+1)/2}\lambda_0 \text{ 是一个平方数}\pmod p & \text{如果 } b \text{ 为偶数,}\\ (-1)^{(v+1)/2}n_0\lambda_0 \text{ 是一个平方数}\pmod p & \text{如果 } b \text{ 为奇数.}\end{cases}$$

为了证明定理 29.3，我们首先证明两个命题.

给定任何一个 $m\times m$ 整数矩阵 $A$，我们可以考虑由其行的所有整数线性组合构成的$\mathbb{Z}$-模 $M(A)$，这就是

$$M(A):=\{\boldsymbol{y}A:\boldsymbol{y}\in\mathbb{Z}^m\}.$$

固定一个素数 $p$，对任意一个正整数 $i$ 定义模

$$M_i:=\{\boldsymbol{x}\in\mathbb{Z}^m: p^i\boldsymbol{x}\in M(A)\},$$

$$N_i:=\{\boldsymbol{y}\in\mathbb{Z}^m: A\boldsymbol{y}^\top\equiv 0 \pmod{p^{i+1}}\}.$$

398

我们有 $M_0=M(A)$；对所有的 $i$，$M_i\subseteq M_{i+1}$且 $N_i\supseteq N_{i+1}$. 设

$$G_i:=M_i \pmod p,\qquad D_i:=N_i \pmod p. \tag{29.1}$$

这就是说，读出 $M_i$ 或 $N_i$ 中的所有整数向量模 $p$ 得到 $C_i$ 或 $D_i$. 则每个 $C_i$ 和 $D_i$ 是向量空间$\mathbb{F}_p^m$的子空间，即 $p$ 元线性码. 显然

$$C_0\subseteq C_1\subseteq C_2\subseteq\cdots \quad 且 \quad D_0\supseteq D_1\supseteq D_2\cdots.$$

**命题 29.4**　*对所有非负的整数 $i$，我们有*

$$C_i^\perp=D_i.$$

**证明**　设 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是整数向量，使得 $\boldsymbol{x}\pmod p\in C_i$ 且 $\boldsymbol{y}\pmod p\in D_i$. 这意味着对某些整数向量 $\boldsymbol{a}$，$\boldsymbol{b}$ 和 $\boldsymbol{z}$ 有

$$p^i(\boldsymbol{x}+p\boldsymbol{a})=\boldsymbol{z}A \quad 和 \quad A(\boldsymbol{y}+p\boldsymbol{b})^\top\equiv 0 \pmod{p^{i+1}}.$$

则

$$p^i(x+pa)\cdot(y+pb)^\top = zA(y+pb)^\top \equiv 0 \pmod{p^{i+1}},$$

这意味着在$\mathbb{F}_p$上$x\cdot y^\top=0$.

我们通过说明$C_i$和$D_i$的维数加起来为$m$完成命题的证明. 存在幺模矩阵$E$和$F$(有整数逆的整数矩阵)使得$S:=EAF$是对角线上为整数$d_1, d_2, \cdots, d_m$的对角矩阵，这些项相继能被前者整除：$d_1 \mid d_2 \mid \cdots \mid d_m$. ($S$是$A$的史密斯(Smith)规范型且$d_i$为$A$的不变因子.)读者应验证模$M_i$和$N_i$在通过应用幺模变换从一个能得到另一个的意义上分别等价于

$$M_i':=\{x: p^ix\in M(S)\} \quad 和$$

$$N_i':=\{y: Sy^\top\equiv 0 \pmod{p^{i+1}}\},$$

因此在$\mathbb{F}_p$上$M_i$和$M_i'$的维数，以及$N_i$和$N_i'$的维数相等. 399

假设$p^{i+1}$不整除$d_1,\cdots,d_t$但整除$d_{t+1},\cdots,d_m$. 那么$y\in N_i'$蕴涵$y$的前$t$个坐标能被$p$整除，前$t$个坐标为零的任何一个向量$y$在$N_i'$中. 因此$N_i'(\text{mod } p)$是后$m-t$个标准基向量的生成，且有维数$m-t$. $x\in M_i'$也蕴涵$x$的最后$d-t$个坐标能被$p$整除，稍加思索即可证明$M_i'(\text{mod } p)$是前$t$个标准基向量的生成且有维数$t$. ■

**命题 29.5** 设$A$，$B$和$U$是满足

$$ABA^\top = nU \tag{29.2}$$

的$m\times m$整数矩阵，这里$U$和$B$是模素数$p$非奇异的. $n$写成$n=p^en_0$，这里$(p, n_0)=1$. 如在(29.1)中那样从$A$定义$p$元码的序列$C_i$. 则$C_e=\mathbb{F}_p^m$且

$$C_i^B = C_{e-i-1}, \quad i=0,1,\cdots,e-1.$$

特别地，如果$e$是奇数，则$C_{\frac{1}{2}(e-1)}$相对于由$B$在$\mathbb{F}_p^m$上给出的标量积是一个自对偶$p$元码.

**证明** 设$x$和$y$是使得$x(\text{mod } p)\in C_i$且$y(\text{mod } p)\in C_{e-i-1}$的整数向量，这意味着对某些整数向量$z_1$，$z_2$，$a_1$和$a_2$，有

$$p^i(x+pa_1)=z_1A \quad 和 \quad p^{e-i-1}(y+pa_2)=z_2A.$$

则由(29.2)，

$$p^{e-1}\langle x,y\rangle = p^{e-1}xBy^\top \equiv z_1ABA^\top z_2^\top \equiv 0 \pmod{p^e}.$$

因此在$\mathbb{F}_p$中$\langle x, y\rangle=0$，我们看出$C_{e-i-1}\subseteq C_i^B$.

现在设$x\in C_i^B$. 这意味着$xB\in C_i^\perp$，由命题29.4，$C_i^\perp$是$D_i$，因此对某个整数向量$x'$，当模$p$时$x'$约化为$x$，

$$x'BA^\top\equiv 0 \pmod{p^{i+1}}. \quad 400$$

由(29.2)，$A\cdot BA^\top U^{-1}=nI$，因为一个矩阵与其逆可交换，

$$BA^\top U^{-1}\cdot A = nI. \tag{29.3}$$

因为$U$模$p$是幺模的，$dU^{-1}$对与$p$互素的某个$d$是整数，例如，$d:=\det(U)$. (29.3)左乘$dx'$得到

$$x'BA^\top(dU^{-1})A = p^edn_0x',$$

那么

$$zA = p^{e-i-1}dn_0x',$$

这里$z:=\frac{1}{p^{i+1}}x'BA^\top(dU^{-1})$是整数. 这意味着$p^{e-i-1}dn_0x'$在$M_{e-i-1}$中，因此$x\in C_{e-i-1}$.

断言 $C_e=\mathbb{F}_p^m$ 作为一个简单的问题留给读者. ■

**问题 29B** 证明 $C_e=\mathbb{F}_p^m$.

**定理 29.3 的证明** 设 $N$ 为一个对称的 $(v, k, \lambda)$-设计的关联矩阵且 $p$ 为一个素数. 假设 $\lambda=p^{2a}\lambda_0$，这里 $(\lambda_0, p)=1$ 且 $a\geqslant 0$；后面我们将解释当 $\lambda$ 恰能被 $p$ 的一个奇数次幂整除时怎么做. 设

$$A:=\begin{bmatrix} & & & p^a \\ & N & & \vdots \\ & & & p^a \\ p^a\lambda_0 & \cdots & p^a\lambda_0 & k \end{bmatrix}, \quad B:=\begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & -\lambda_0 \end{bmatrix}. \tag{29.4}$$

读者应利用 $N$ 的性质和关系 $\lambda(v-1)=k(k-1)$ 验证 $ABA^\top=nB$.

在 $\lambda$ 恰能被 $p$ 的偶数次幂整除时，应用命题 29.5，以及如同在(29.4)中给出的矩阵 $A$ 和 $B$，这里 $U:=B$.

当 $\lambda$ 恰能被 $p$ 的奇数次幂整除时，我们把上面的情形用于给定的对称设计的补，即一个对称的 $(v, v-k, \lambda')$-设计，这里 $\lambda'=v-2k+\lambda$. 比如说 $\lambda'=p^c\lambda_0'$，这里 $(\lambda_0', p)=1$. 从 $\lambda\lambda'=n(n-1)$，得出 $c$ 是奇数且

401

$$\lambda_0\lambda_0'=n_0(n-1)\equiv -n_0 \pmod p.$$

在结论中本来是 $-\lambda_0'$ 的地方我们已换为 $\lambda_0 n_0$，这是允许的，原因是为了用原来的参数表示结果，它们相差模 $p$ 的一个平方因子. ■

下面的定理是问题 19M 的一个结论，但我们给出与定理 29.3 类似的证明.

**定理 29.6** *如果存在一个阶 $n\equiv 2 \pmod 4$ 的会议矩阵，则没有素数 $p\equiv 3 \pmod 4$ 能整除 $n-1$ 的无平方因子部分.*

**证明** 一个阶为 $n$ 的会议矩阵是使得 $AA^\top=(n-1)I_n$ 的整数矩阵 $A$. 在 $A=U=I$ 时，由命题 29.5，对 $n-1$ 的无平方因子部分的每一个素因子 $p$，存在一个长度为 $n$ 的自对偶 $p$ 元码(相对于标准内积的自对偶). 定理 29.2 蕴涵每个这样的素数是 $\equiv 1 \pmod 4$. ■

* * *

当 $p$ 不能整除交换群 $G$ 的阶 $v$ 时，群环 $\mathbb{F}_p[G]$ 是 $\mathbb{F}_p=\mathbb{Z}_p$ 上的半-简单的代数. 这意味着不存在非零的幂零元，即对某个正整数 $m$，非零元素 $a$ 使得 $a^m=0$. 非零的幂零元的不存在性在引理 28.5 中证明. 由韦德伯恩(Wedderburn)定理，域 $\mathbb{F}$ 上每个有单位元的有限维交换的半-简单代数 $\mathcal{A}$ 同构于域的直积，这些域中的每一个都是 $\mathbb{F}$ 的扩张. 由此得出，$\mathcal{A}$ 的每一个理想 $\mathcal{I}$ 是主理想，且是由一个幂等元，即满足 $e^2=e$ 的元素 $e$ 生成的. 证明可参见任意一本关于代数学的高深著作.

我们并不需要有关这一信息的方方面面，但这里是我们需要的由幂等元生成的主理想的有关事实. 这些问题是好的练习.

首先，如果 $\mathcal{I}=\langle e_1\rangle$ 且 $\mathcal{I}=\langle e_2\rangle$，这里 $e_1$ 和 $e_2$ 都是幂等元，则 $e_1=e_2$. 假设 $\mathcal{I}_1=\langle e_1\rangle$，$\mathcal{I}_2=\langle e_2\rangle$，这里 $e_1$ 和 $e_2$ 都是幂等元，则

$$\mathcal{I}_1\cap\mathcal{I}_2=\langle e_1e_2\rangle \quad 和 \quad \mathcal{I}_1+\mathcal{I}_2=\langle e_1+e_2-e_1e_2\rangle.$$

注意 $e_1e_2$ 和 $e_1+e_2-e_1e_2$ 仍是幂等元. 402

**定理 29.7** 设 $D$ 是阶为 $v:=n^2+n+1$ 的交换群 $G$ 中的一个$(n^2+n+1, n+1, 1)$-差集. 如果 $n\equiv 0 \pmod 2$但 $n\not\equiv 0 \pmod 4$, 则 $n=2$. 如果 $n\equiv 0 \pmod 3$但 $n\not\equiv 0 \pmod 9$, 则 $n=3$.

**证明** 设 $D$ 是交换群 $G$ 中的一个$(n^2+n+1, n+1, 1)$-差集, 并设 $p$ 为 $n$ 的一个素因子. 由定理 28.3, $p$ 是 $D$ 的一个乘子, 从现在起假定 $D$ 被 $p$ 固定. 这里以$\mathbb{F}_p$-代数$\mathbb{F}_p[G]$为例进行讨论.

设$\mathcal{I}_1$ 是$\mathbb{F}_p[G]$中由 $D(x)$生成的理想且$\mathcal{I}_2$ 是由 $D(x^{-1})$生成的理想.

我们有 $D(x^p)=D(x)$, 但由引理 28.2 知 $D^p(x)=D(x^p)$, 因此在$\mathbb{F}_p[G]$中 $D^p(x)=D(x)$. 则 $D^{p-1}(x)$是幂等的且也生成$\mathcal{I}_1$. 类似地, $D^{p-1}(x^{-1})$是$\mathcal{I}_2$ 的一个幂等生成元. 因此$\mathcal{I}_1\cap\mathcal{I}_2$ 的幂等生成元是

$$D^{p-1}(x)D^{p-1}(x^{-1}) = (n+G(x))^{p-1} = G(x),$$

$\mathcal{I}_1+\mathcal{I}_2$ 的幂等生成元是

$$D^{p-1}(x)+D^{p-1}(x^{-1})-G(x).$$

现在我们希望考虑$\mathbb{F}_p$ 上的$\mathcal{I}_1$ 和$\mathcal{I}_2$ 的维数. 一般地, 由 $A(x)$生成的主理想的秩是一个 $v\times v$ 矩阵的秩, 该矩阵的行是 $x^gA(x)$的系数, $g\in G$. 当 $A(x)=D(x)$或 $D(x^{-1})$时, 这个矩阵是一个对称的$(n^2+n+1, n+1, 1)$-设计的关联矩阵. 如果现在我们假设 $p^2$ 不整除 $n$, 则由定理 29.1, $\mathcal{I}_1$ 和$\mathcal{I}_2$ 的维数为$(v+1)/2$. 交$\mathcal{I}_1\cap\mathcal{I}_2$ 的维数为 1, 因此它们的和有维数 $v$. 整个群环本身作为一个理想的幂等生成元是 1, 因此我们有结论: 在$\mathbb{F}_p[G]$中,

$$D^{p-1}(x)+D^{p-1}(x^{-1})-G(x) = 1. \tag{29.5}$$

仅能在 $p=2$ 或 3 时利用上面的等式. 当 $p=2$ 时, (29.5)断言在$\mathbb{Z}[G]$中 $D(x)+D(x^{-1})\equiv 1+G(x) \pmod 2$, $1+G(x)$的奇数系数的数目是 $v-1=n^2+n$, 但 $D(x)+D(x^{-1})$的奇数系数的数目不能超过 $2(n+1)$, 因此 $n\leqslant 2$. 403

当 $p=3$ 时, (29.5)断言在$\mathbb{Z}[G]$中 $D^2(x)+D^2(x^{-1})\equiv 1+G(x) \pmod 3$. 我们断定 $D^2(x)$和 $D^2(x^{-1})$的非零系数由 $n+1$ 个 1 和$\binom{n+1}{2}$个 2 构成. 如果 $C$ 是任何一个平面差集, 则对每个 $g\in G$ 在 $C^2(x)$中存在一项 $x^{2g}$且对每个无序对$\{g, h\}\subseteq C$ 存在一项 $2x^{g+h}$; 注意 $\lambda=1$ 蕴涵着, 例如 $g_1+h_1\neq g_2+h_2$, 除非$\{g_1, h_1\}=\{g_2, h_2\}$. 两个这样的群环的元素之和不能有多于$\binom{n+2}{2}+2(n+1)$个系数$\equiv 1 \pmod 3$, 但 $1+G(x)$有 $n^2+n$ 个系数等于 1, 由此得出 $n\leqslant 4$. ■

**问题 29C** 设 $D$ 是一个满足 $n\equiv 2 \pmod 4$的差集且 2 是 $D$ 的一个乘子, 作为 $n$ 的函数, $D$ 的参数是什么?

## 评注

对定理 29.3 的证明之前的一些材料, 如果引入 $p$-adic 数会更简洁, 如在 Lander(1983)中那样, 但我们选择的内容不包含它们.

## 参考文献

D. Jungnickel and K. Vedder (1984), On the geometry of planar difference sets, *European J. Combinatorics* **5**, 143–148.

E. S. Lander (1983), *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lecture Note Series **74**, Cambridge University Press.

V. Pless (1986), Cyclic projective planes and binary extended cyclic self-dual codes, *J. Combinatorial Theory* (A) **43**, 331–333.

H. A. Wilbrink (1985), A note on planar difference sets, *J. Combinatorial Theory* (A) **38**, 94–95.

404

# 第30章 结合方案

给定一个 $n$-集合的两个 $k$-子集，其中 $n \geqslant 2k$，它们之间存在 $k+1$ 种可能的关系：它们可能相等，可能交于 $k-1$ 个元素，可能交于 $k-2$ 个元素，…，或者可能不相交.

给定两个字($k$ 元组)$\boldsymbol{a}$，$\boldsymbol{b} \in A^k$，这里 $A$ 是规模至少为 2 的一张“字母表”，它们之间有 $k+1$ 种可能的关系：它们可能相等，可能 $k-1$ 个坐标相符，可能 $k-2$ 个坐标相符，…，或者所有的坐标都不相符.

一个集合与相互排斥且穷尽的二元关系的这些例子是下面要定义的*结合方案*的特例. 结合方案提供了组合学的基础之一，因此即使难读我们也把它包括在本章之中. 它们已隐含在前面的许多章中；我们已明确地讨论过 2-类结合方案，它们等价于第 21 章讨论的强正则图. 本章详述第 21 章的一些材料但目的不同.

结合方案首先出现在实验设计的统计理论中，但 Ph. Delsarte(1973)已经证明它们怎样用于统一我们主题的许多方面. 特别地，编码理论和 $t$-设计理论的某些结果——它们当初是独立发现的——现在看来是结合方案中同一思想的“形式上对偶的”表现. 例如，费希尔不等式及其推广(即定理 19.8)与球装填的界(即定理 21.1)是形式上对偶的. 在本章中我们用结合方案的机制给出关于完全码的 Lloyd 定理及其形式对偶定理的证明，这个形式对偶定理是关于紧设计和正交阵列的. Delsarte 不等式，即关于结合方案的一个子集的分布向量的定理 30.3，关于码的规模提供了一个“线性规划界”，而且对极值集合论也有用处.



一个集合 $\mathfrak{X}$ 上的*二元关系*，是指 $\mathfrak{X} \times \mathfrak{X}$ 的一个子集. 点集 $\mathfrak{X}$ 上的一个 *$k$-类结合方案*，有时我们仅说*方案*，由 $\mathfrak{X}$ 上 $k+1$ 个非空的对称二元关系 $R_0$，$R_1$，…，$R_k$ 组成，它们划分 $\mathfrak{X} \times \mathfrak{X}$，这里 $R_0 = \{(x, x) : x \in \mathfrak{X}\}$是恒等关系，并且对某个非负整数 $p_{ij}^{\ell}$，$0 \leqslant \ell$，$i$，$j \leqslant k$，使得如下的公理系统成立：给定任意一个$(x, y) \in R_{\ell}$，恰好存在 $p_{ij}^{\ell}$ 个元素 $z \in \mathfrak{X}$ 使得$(x, z) \in R_i$ 且$(z, y) \in R_j$. 当$(x, y) \in R_i$ 时，我们说 $x$，$y \in \mathfrak{X}$ 是*第 $i$ 次结合*.

数 $p_{ij}^{\ell}$($0 \leqslant \ell$，$i$，$j \leqslant k$)是该方案的*参数*. $p_{ii}^{0}$存在意味着 $\mathfrak{X}$ 的任意一个元素的第 $i$ 次结合存在一个常数，该常数通常用 $n_i$ 表示. 我们有

$$p_{ii}^{0} = n_i \quad 且 \quad p_{ij}^{0} = 0 \quad 对 \quad i \neq j \tag{30.1}$$

以及

$$n_0 = 1, n_0 + n_1 + \cdots + n_k = N.$$

这里 $N := |\mathfrak{X}|$. 数 $n_0$，$n_1$，…，$n_k$ 称为该方案的*度*.

**例 30.1** 约翰逊(Johnson)方案 $J(v, k)$. $J(v, k)$的点是一个 $v$-集合 $S$ 的$\binom{v}{k}$个 $k$-子集. 当 $|A \cap B| = k-i$ 时，两个 $k$-子集 $A$，$B$ 被说成是第 $i$ 次结合. 于是 0 次结合是相等. “由对称性”参数 $p_{ij}^{\ell}$存在且可以表示为二项式系数之积的和，但我们不打算一般地写出这些表示.

例如，方案 $J(6, 3)$是 20 个点的 3-类方案. 读者应检查 $n_1 = n_2 = 9$，$n_3 = 1$. 其他参数中的几个是 $p_{11}^{1} = 4$，$p_{11}^{2} = 4$，$p_{11}^{3} = 0$.

**例 30.2** 汉明方案 $H(n, q)$. $H(n, q)$的点是规模为 $q$ 的一张字母表上的长度为 $n$ 的 $q^n$ 个字. 当两个字 $x$ 和 $y$ 恰在 $i$ 个坐标上不相同时，说这两个 $n$ 元组 $x$，$y$ 是第 $i$ 次结合. 于是 0 次结合是相等. “由对称性”参数 $p_{ij}^{\ell}$ 存在且可以表示为二项式系数及 $q-1$ 的幂之积的和，我们不打算一般地写出这些表示. [406]

例如，方案 $H(5, 3)$是 125 个点的 5-类方案. 读者应检查 $n_1=5\cdot 2$，$n_2=10\cdot 4$，等等.

关系 $R_i$ 中的每一个可以想象为点集 $\mathfrak{X}$ 上的一个图 $G_i$ 的邻接关系. (一个方案是完全图的边的一类特殊的划分——或者边的染色.) 如果我们以一个 2-类方案开始，则 $G_1$ 是一个度为 $n_1$ 的强正则图，$\lambda=p_{11}^1$ 且 $\mu=p_{11}^2$. 事实上，当我们宣称 $G$ 中两个不同的顶点相邻时它们是第 1 次结合，当它们不相邻时是第 2 次结合，则任意强正则图给出一个 2-类结合方案；其他参数存在，即它们是常数并且能从该图的参数中算出. 例如，$p_{12}^1=k-\lambda-1$.

一个图 $G$ 是*距离正则图*，如果到 $x$ 的距离为 $i$ 的顶点的数目和到 $y$ 的距离为 $j$ 的顶点的数目仅与顶点 $x$ 和 $y$ 之间的距离有关，而不是与特殊的顶点有关. 这就是，定义两个顶点是第 $i$ 次结合当且仅当在 $G$ 中它们的距离是 $i$ 产生一个结合方案(这里类的数目是图的直径). 见 Brouwer, Cohen, and Neumaier(1989). 以这种方式产生的方案称为*度量的*. 上面例 30.1 和例 30.2 提到的方案是度量的，下面例 30.3 和例 30.4 中的方案也是度量的.

知道参数 $p_{ij}^{\ell}$ 存在是重要的，但知道它们的精确值并不那么重要. 这是一种幸运，因为通常给不出这些参数的方便表示. 例如，在方案 $J(v, k)$中，对一般的 $p_{ij}^{\ell}$，似乎需要二项式的一个三项和. 在前面刚刚给出的例子中，我们知道 $p_{ij}^{\ell}$ 存在是由于“对称”，更精确一些，在每一种情形存在 $\mathfrak{X}$ 的一个置换群 $G$ 使得两个有序点对$(x_1, y_1)$和$(x_2, y_2)$在同一个关系 $R_i$ 中，当且仅当存在 $\sigma\in G$ 使得 $\sigma(x_1)=x_2$ 且 $\sigma(y_1)=y_2$. 这就是，关系 $R_0$，$R_1$，…，$R_k$ 是 $G$ 在 $\mathfrak{X}\times\mathfrak{X}$ 上的轨道($R_0$ 是所有$(x, x)$的轨道，$x\in\mathfrak{X}$). 在例 30.1 中，$G$ 是作用在一个 $v$-集合的所有 $k$-子集上的对称群 $S_v$，我们可以找到一个把 $k$-子集的一个有序对变成另一个有序对的置换，当且仅当每个有序对的交的规模相同. 在例 30.2 中，$G$ 是带 $S_n$ 的 $S_q$ 的圈积(这就是，我们允许 $n$ 个坐标的任何置换跟着每个坐标上 $q$ 个符号的无关的置换)；可以找到把 $n$ 元组的一个有序对变成另一个有序对的这样一个变换，当且仅当两个有序对的坐标的数目相同. [407]

一般地，如果一个集合 $\mathfrak{X}$ 上置换的可迁群 $G$ 使得 $G$ 在 $\mathfrak{X}\times\mathfrak{X}$ 上的轨道是对称的，则它们可能被取作 $\mathfrak{X}$ 上的一个结合方案的关系. 下面的三个例子来自这种方式.

**例 30.3** 这是约翰逊方案的 $q$-类似：取$\mathbb{F}_q$ 上的一个 $v$-空间 $V$ 的 $k$-子空间作为点. 当 $\dim(A\cap B)=k-i$ 时，称两个 $k$-子空间 $A$ 和 $B$ 是第 $i$ 次结合.

**例 30.4** 比如说取$\mathbb{F}_q$ 上的 $k\times m$ 矩阵作为点，这里 $k\leqslant m$. 当 $A-B$ 的秩是 $k-i$ 时，称两个矩阵 $A$ 和 $B$ 是第 $i$ 次结合.

为了把这个例子放到上面的框架中，我们设 $\mathfrak{X}$ 是所有 $k\times m$ 矩阵的集合，取 $G$ 是所有置换 $X\mapsto UXW+C$ 的集合，其中 $U$ 遍历非奇异 $k\times k$ 矩阵，$W$ 遍历非奇异 $m\times m$ 矩阵，且 $C$ 遍历 $k\times m$ 矩阵. 如果$(A, B)$和$(A', B')$是使得 $A-B$ 的秩和 $A'-B'$的秩相同的 $k\times m$ 矩阵的对子，则对某些非奇异矩阵 $U$ 和 $W$，$U(A-B)W=A'-B'$，且 $X\mapsto UXW+(B'-UBW)$把第一对矩阵映射到第二对.

**例 30.5** 得到割圆方案如下. 设 $q$ 是一个素数的幂且 $k$ 是 $q-1$ 的一个因子. 设 $C_1$ 是 $\mathbb{F}_q$ 的乘法群的一个子群其指标为 $k$, 又设 $C_1$, $C_2$, …, $C_k$ 是 $C_1$ 的陪集. 方案的点是 $\mathbb{F}_q$ 的元素, 当 $x-y\in C_i$ 时, 称两个点 $x$ 和 $y$ 是第 $i$ 次结合(当 $x-y=0$ 时是 0 次结合). 为了按上面的定义得到一个方案, 我们需要 $-1\in C_1$, 因此关系将是对称的, 即如果 $q$ 是奇数, $2k$ 一定整除 $q-1$, 例 21.3 是 $k=2$ 的情形. [408]

我们引入结合方案的结合矩阵 $A_0$, $A_1$, …, $A_k$(也称邻接矩阵). 这些矩阵是方阵, 其行和列由一个方案的点集 $\mathfrak{X}$ 的元素指示. 对 $i=0$, 1, …, $k$, 我们定义

$$A_i(x,y)=\begin{cases}1 & \text{如果}(x,y)\in R_i,\\ 0 & \text{否则}.\end{cases}$$

矩阵 $A_i$ 是对称的(0, 1)-矩阵且

$$A_0=I,\quad A_0+A_1+\cdots+A_k=J,$$

这里 $J$ 是 $N\times N$ 的全幺矩阵. 我们用 $\mathfrak{A}$ 表示 $A_0$, $A_1$, …, $A_k$ 的实向量上的线性生成. 这些矩阵是线性无关的, 因为每个矩阵至少包含一个 1, 且在 $A_i$ 中有一个位置有 1, 而在其他结合矩阵的这个位置上是 0. 结合方案的公理恰好是那些保证 $\mathfrak{A}$ 在矩阵乘法下封闭的条件. 为明白这一点, 只要证明任意两个基矩阵的积在 $\mathfrak{A}$ 中就够了, 事实上, 我们有

$$A_iA_j=\sum_{\ell=0}^{k}p_{ij}^{\ell}A_\ell, \tag{30.2}$$

因为 $A_iA_j(x, y)$是使得 $A_i(x, z)=1$ 且 $A_j(z, y)=1$ 的 $z$ 的数目, 而且这个数目是 $p_{ij}^{\ell}$, 这里的 $\ell$ 使得 $A_\ell(x, y)=1$.

代数 $\mathfrak{A}$ 称为方案的 Bose-Mesner 代数; 第 21 章中针对强正则图引入了这个代数. 注意, $\mathfrak{A}$ 不仅在正常的矩阵乘法下封闭, 而且在问题 21E 中引入的阿达马乘法下封闭. 两个矩阵的阿达马积 $A\circ B$ 是由按坐标乘法

$$(A\circ B)(x,y):=A(x,y)B(x,y)$$

得到的矩阵. [409]

作为关于阿达马乘法的一个代数, $\mathfrak{A}$ 几乎是平凡的. 我们有

$$A_i\circ A_j=\begin{cases}A_i & \text{如果 } i=j,\\ O & \text{如果 } i\neq j\end{cases}$$

(这就是, $A_0$, $A_1$, …, $A_k$ 是正交幂等元), $A_i$ 的和是 $J$, 即关于阿达马乘法的单位元. 因此, 当 $\mathfrak{A}$ 中的矩阵用相对于 $\mathfrak{A}$ 的基 $A_0$, $A_1$, …, $A_k$ 表示时, 阿达马乘法特别简单.

然而, 矩阵理论中一个众所周知的结果(谱定理的推广, 谱定理说一个对称的实矩阵有一组特征向量作为正交基)断言实对称矩阵的一个交换代数相对于通常的矩阵乘法有一组正交的幂等基, 基向量之和等于单位元. 更几何化一些, 欧几里得空间$\mathbb{R}^{\mathfrak{X}}$存在一个正交分解

$$\mathbb{R}^{\mathfrak{X}}=V_0\oplus V_1\oplus\cdots\oplus V_k,$$

$\mathbb{R}^{\mathfrak{X}}$是其坐标由 $\mathfrak{X}$ 的元素指示的所有向量的空间, 内积为标准的内积, 使得从$\mathbb{R}^{\mathfrak{X}}$分别映上到 $V_0$, $V_1$, …, $V_k$ 的正交射影 $E_0$, $E_1$, …, $E_k$ 为 $\mathfrak{A}$ 的一组基. 我们有

$$E_iE_j=\begin{cases}E_i & 如果\ i=j,\\ O & 如果\ i\neq j,\end{cases}$$

且

$$E_0+E_1+\cdots+E_k=I.$$

当然，当矩阵相对于基 $E_0$，$E_1$，…，$E_k$ 被表出时，通常的乘法也特别简单.

子空间 $V_0$，$V_1$，…，$V_k$ 称为方案的特征空间：在一个线性组合 $M=\sum_{i=0}^{k}\lambda_iE_i$ 中，$V_i$ 中的每个向量对 $M$ 是值 $\lambda_i$ 的一个特征向量. 一般地特征空间没有自然的编号，除了一种例外：因为 $J\in\mathfrak{A}$，$J$ 有全幺的向量 $\boldsymbol{j}$ 作为值 $N$ 的一个特征向量且所有与 $\boldsymbol{j}$ 正交的向量作为值 0 的特征向量，所以必定有一个特征空间仅由 $\boldsymbol{j}$ 的标量倍数组成——我们总假设这个空间是 $V_0$. 则到 $V_0$（它有 $\boldsymbol{j}$ 作为值 1 的特征向量且所有与 $\boldsymbol{j}$ 正交的向量作为值 0 的特征向量）的正交射影是 [410]

$$E_0=\frac{1}{N}J.$$

令 $m_i$ 表示 $V_i$ 的维数. 则

$$m_0=1,\quad m_0+m_1+\cdots+m_k=N.$$

注意 $m_i$ 是 $E_i$ 的迹，因为 $E_i$ 的特征值是 1（重数等于 $V_i$ 的维数）和 0. 数 $m_0$，$m_1$，…，$m_k$ 是方案的重数.

**例 30.6** 我们可以显式地描述汉明方案 $H(n, 2)$ 的特征空间. 这个方案的点是 $\mathbb{F}_2^n$ 的二元 $n$-数组（或字）$a$.

对每个 $a\in\mathbb{F}_2^n$，由

$$\boldsymbol{v}_a(b):=(-1)^{\langle a,b\rangle}$$

定义其坐标由点集指示的一个向量 $\boldsymbol{v}_a$. 这些向量是正交的且是一个阿达马矩阵的行，见图 30.1和第 18 章. 我们断言 $V_i$ 可以取作所有向量 $\boldsymbol{v}_a$ 的生成，$\boldsymbol{v}_a$ 的 $a$ 遍历重量为 $i$（$i=0$，1，…，$n$）的字.

$$\begin{bmatrix}1&1&1&1&1&1&1&1\\1&-1&1&1&1&-1&-1&-1\\1&1&-1&1&-1&1&-1&-1\\1&1&1&-1&-1&-1&1&-1\\1&1&-1&-1&1&-1&-1&1\\1&-1&1&-1&-1&1&-1&1\\1&-1&-1&1&-1&-1&1&1\\1&-1&-1&-1&1&1&1&-1\end{bmatrix}$$

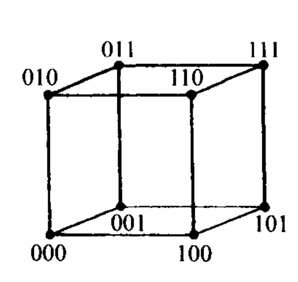



图 30.1

我们验证每个 $\boldsymbol{v}_a$ 是所有结合矩阵 $A_j$ 的一个特征向量. 设 $a$ 的重量为 $\ell$. 则

$$\begin{aligned}(\boldsymbol{v}_aA_j)(b)&=\sum_{c}\boldsymbol{v}_a(c)A_j(c,b)\\&=\sum_{c:d(b,c)=j}(-1)^{\langle a,c\rangle}=(-1)^{\langle a,b\rangle}\sum_{c:d(b,c)=j}(-1)^{\langle a,b+c\rangle}\end{aligned}$$

$$= \boldsymbol{v}_a(b) \sum_{u: \mathrm{wt}(u)=j} (-1)^{\langle a,u\rangle} = \boldsymbol{v}_a(b) \sum_{i=0}^{n} (-1)^i \binom{\ell}{i}\binom{n-\ell}{j-i}.$$

这一计算证明，当 $E_i$ 是到 $V_i$ 的正交射影的矩阵时，

$$A_j = \sum_{\ell=0}^{n}\left(\sum_{i=0}^{n}(-1)^i\binom{\ell}{i}\binom{n-\ell}{j-i}\right)E_\ell,$$

411

这是因为当两边乘以任何一个 $\boldsymbol{v}_a$ 时给出相同的结果. 因此 $\mathfrak{A} \subseteq \mathrm{span}\{E_0, \cdots, E_n\}$. 等号成立是因为两个空间的维数都是 $n+1$.

方案 $H(n, q)$ 对一般 $q$ 的特征值在下面的定理 30.1 中给出.

例如，如果把长度 $n=3$ 的字排序为

$$000,100,010,001,011,101,110,111,$$

则图 30.1 右侧显示的立方体（$=H(3, 2)$ 中的 $A_1$）的特征空间 $V_0$，$V_1$，$V_2$，$V_3$ 分别由图 30.1 左侧的阿达马矩阵的第一行、接下来的三行、再接下来的三行、最后一行生成.

**例 30.7** 下面描述约翰逊方案 $J(v, k)$ 的特征空间，但略去证明，见 Delsarte(1973) 或 Wilson(1984b).

这个方案的点集是一个 $v$-集合 $X$ 的 $k$-子集 $S$ 的集合 $\mathfrak{X}$. 对每个规模 $\leqslant k$ 的子集 $T \subseteq X$，设 $\boldsymbol{e}_T$ 是 $\mathbb{R}^{\mathfrak{X}}$ 中长度为 $\binom{v}{k}$ 的向量，这里

$$\boldsymbol{e}_T(S) := \begin{cases} 1 & \text{如果 } T \subseteq S, \\ 0 & \text{其他.} \end{cases}$$

对 $i=0, 1, \cdots, k$，设 $U_i$ 是 $\{\boldsymbol{e}_T : T \subseteq X, |T| = i\}$ 的生成，我们断言 $U_0 \subseteq U_1 \subseteq \cdots \subseteq U_k = \mathbb{R}^{\mathfrak{X}}$ 且 $U_i$ 的维数为 $\binom{v}{i}$. 设 $V_0 := U_0$（常数向量）且对 $i>0$，设 $V_i$ 是 $U_i$ 中 $U_{i-1}$ 的正交补，即

$$V_i := U_i \cap U_{i-1}^{\perp}.$$

412

显然 $V_0$，$V_1$，$\cdots$，$V_k$ 正交且和为 $\mathbb{R}^{\mathfrak{X}}$. 可以证明 $V_i$ 中的每个向量是值为 $P_j(i)$ 的 $A_j$ 的一个特征向量，正如在下面定理 30.1(i) 所显示的.

因为我们有向量空间 $\mathfrak{A}$ 的两组基，所以可以考虑它们之间的变换矩阵，称之为方案的**特征矩阵**. 定义 $P$（第一个特征矩阵）和 $Q$（第二个特征矩阵）为行和列由 0，1，$\cdots$，$k$ 指示的 $(k+1)\times(k+1)$ 矩阵，使得

$$(A_0, A_1, \cdots, A_k) = (E_0, E_1, \cdots, E_k)P$$

且

$$N(E_0, E_1, \cdots, E_k) = (A_0, A_1, \cdots, A_k)Q.$$

$P$ 的 $(i, \ell)$ 项写作 $P_\ell(i)$，类似地，$Q$ 的 $(i, \ell)$ 项写作 $Q_\ell(i)$，所以

$$A_\ell = P_\ell(0)E_0 + P_\ell(1)E_1 + \cdots + P_\ell(k)E_k, \tag{30.3}$$

且

$$NE_\ell = Q_\ell(0)A_0 + Q_\ell(1)A_1 + \cdots + Q_\ell(k)A_k. \tag{30.4}$$

当然，我们有

$$Q = NP^{-1}, \quad P = NQ^{-1}.$$

$P$ 的第 $\ell$ 列由 $A_\ell$ 的特征值组成.

而知道一个方案的参数 $p_{ij}^{\ell}$ 并不重要，在应用中重要的是知道特征矩阵 $P$ 和 $Q$. 对下面定理的证明及其他方案的特征矩阵的确定，见 Bannai and Ito(1984)或者 Delsarte(1973).

**定理 30.1** (i)对约翰逊方案 $J(v, k)$，其度是 $n_\ell=\binom{k}{\ell}\binom{v-k}{\ell}$ 且重数是 $m_\ell=\binom{v}{\ell}-\binom{v}{\ell-1}$，$\ell=0, 1, \cdots, k$. 第一个特征矩阵的项是 $P_\ell(i)$，这里

413

$$P_\ell(x) = \sum_{\alpha=0}^{\ell}(-1)^{\ell-\alpha}\binom{k-\alpha}{\ell-\alpha}\binom{k-x}{\alpha}\binom{v-k+\alpha-x}{\alpha}.$$

(ii)对汉明方案 $H(n, q)$，其度和重数是 $n_\ell=m_\ell=\binom{n}{\ell}(q-1)^\ell$，$\ell=0, 1, \cdots, n$. 第一个特征矩阵的项是 $P_\ell(i)$，这里

$$P_\ell(x) = \sum_{\alpha=0}^{\ell}(-q)^\alpha(q-1)^{\ell-\alpha}\binom{n-\alpha}{\ell-\alpha}\binom{x}{\alpha}.$$

**问题 30A** 按如下的方式计算 $J(8, 3)$的特征矩阵 $P$. 首先作为 $A_0$，$A_1$，$A_2$ 和 $A_3$ 的线性组合计算 $A_1A_2$，然后填充下面不完整的行：

$$\begin{aligned}
A_1^0 &= A_0,\\
A_1^1 &= \qquad\quad A_1,\\
A_1^2 &= 15A_0 + 6A_1 + 4A_2,\\
A_1^3 &= \qquad\qquad\qquad\qquad\qquad,\\
A_1^4 &= 1245A_0 + 1036A_1 + 888A_2 + 720A_3.
\end{aligned}$$

从这张表导出 $A_1$ 的极小多项式有些冗长. 寻找 $A_1$ 的特征值. 现在把 $A_2$ 和 $A_3$ 表示成 $A_1$ 的多项式，因此找到它们的特征值. 寻找方案的重数. 通过验证定理 30.2 的正交关系或仅由定理 30.1(i)计算相关的值检验你的结果.

**问题 30B** 给定一个方案的特征矩阵 $P$，说明怎样计算一个方案所有的参数 $p_{ij}^{\ell}$. 这就是，证明它们是由 $P$ 唯一确定的.

**问题 30C** 拉丁方图是 $srg(v, k, \lambda, \mu)$，这里对某些整数 $n$ 和 $r$，

$$v = n^2, \quad k = r(n-1), \quad \lambda = (n-2)+(r-1)(r-2), \quad \mu = r(r-1).$$

对 $r=3$，这些参数已在例 21.7 中引入. 对与这些图对应的 2-类方案，找出特征矩阵 $P$ 和 $Q$.

414

所谓的负拉丁方图是强正则图 $srg(v, k, \lambda, \mu)$，其参数在上面的式子中由 $-n$ 替换 $n$，$-r$ 替换 $r$ 得到. 因此 $v=(-n)^2$，$k=(-r)(-n-1)$，等等. (奇怪的是这应该产生满足(21.4)的参数，但确实如此.)找出与 2-类方案对应的特征矩阵 $P$ 和 $Q$.

**定理 30.2** 一个方案的特征矩阵满足正交关系

$$P^\top\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & m_1 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & 0 & \cdots & m_k\end{bmatrix}P = N\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & n_1 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & 0 & \cdots & n_k\end{bmatrix}$$

及

$$Q^{\top}\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & n_1 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & 0 & \cdots & n_k\end{bmatrix}Q = N\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & m_1 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & 0 & \cdots & m_k\end{bmatrix}.$$

**证明** 向量空间 $\mathfrak{A}$ 可以以有些自然的方式配备内积：定义 $\langle A, B\rangle$ 为阿达马积 $A\circ B$ 的项之和. 检验这与矩阵积 $AB^{\top}$ 的迹是相同的(当然，当 $B$ 对称时，这与 $\mathrm{tr}(AB)$ 是相同的).

相对于这个内积，基 $A_0, A_1, \cdots, A_k$ 是一组正交基(但不是标准正交的)，我们有 $\langle A_i, A_i\rangle = Nn_i$. 但 $E_0, E_1, \cdots, E_k$ 也是一组正交基，因为对 $i\neq j$，$E_iE_j=0$；我们有 $\langle E_i, E_i\rangle=\mathrm{tr}(E_i)=m_i$. 现在从这里导出该定理属于初等线性代数的知识.

考虑第一个关系，在右边 $(\alpha, \beta)$ 位置上的项是

$$\begin{aligned}\langle A_\alpha, A_\beta\rangle &= \Big\langle \sum_i P_\alpha(i)E_i, \sum_j P_\beta(j)E_j\Big\rangle\\ &= \sum_{i,j}P_\alpha(i)P_\beta(j)\langle E_i, E_j\rangle = \sum_i m_iP_\alpha(i)P_\beta(i),\end{aligned}$$

且最后一个表达式是在左边 $(\alpha, \beta)$ 位置上的项. 类似地导出第二个关系. ■ [415]

表示上述定理的另一个方式是

$$Q=\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & n_1 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & 0 & \cdots & n_k\end{bmatrix}^{-1}P^{\top}\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & m_1 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & 0 & \cdots & m_k\end{bmatrix}.$$

等价地，对所有 $i, j=0, 1, \cdots, k$，

$$m_jP_i(j) = n_iQ_j(i). \tag{30.5}$$

由定理 30.1 和定理 30.2，对方案 $J(v, k)$ 和 $H(n, q)$ 可以找到第二个特征矩阵 $Q$. 有些奇怪的是对 $H(n, q)$，$P=Q$，读者应检验这个关系.

**问题 30D** 解释为何 $P$ 和 $Q$ 的第 0 行和第 0 列如下所示：

$$P=\begin{bmatrix}1 & n_1 & \cdots & n_k\\ 0 & & & \\ \vdots & & & \\ 1 & & & \end{bmatrix},\quad Q=\begin{bmatrix}1 & m_1 & \cdots & m_k\\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{bmatrix}. \tag{30.6}$$

Delsarte(1973)观察到第二个特征矩阵 $Q$ 的列提供了一个线性约束系统，我们称之为 Delstarte 不等式，它们作用在他所说的一个非空子集 $Y$ 的"内分布向量"上，$Y$ 是一个结合方案的点集 $\mathfrak{X}$ 的子集. 定义 $Y$ 的分布向量为 $\boldsymbol{a}=(a_0, a_1, \cdots, a_k)$，这里

$$a_i := \frac{1}{|Y|}|(Y\times Y)\cap R_i|;$$

这就是，$a_i$ 是一个元素 $x\in Y$ 的第 $i$ 次结合 $y\in Y$ 的平均数. 我们有

$$a_0 = 1,\quad a_0+a_1+\cdots+a_k = |Y|.$$

对许多有趣的子集 $Y$，一个元素 $x\in Y$ 的第 $i$ 次结合 $y\in Y$ 的数目是常数，即不依赖于 $Y$ 中 $x$ 的选择. 例如，这对 $H(n, q)$ 中的线性码 $C$ 是正确的，在这一情形中分布向量与第 21 章 [416]

中所介绍的 $C$ 的重量计数器重合；这对前几章中我们已讨论过的优美构形也是正确的，它们的分布向量列在下面．这里汉明(7)是长度为 7 的汉明码，“戈莱”是“戈莱码”的简称，“X”指“扩展的”，“ * ”表示“对偶码”.

| 对象 | 方案 | 分布向量 |
|---|---|---|
| $S(2,3,7)$ | $J(7,3)$ | (1,0,6,0) |
| $S_2(2,5,11)$ | $J(11,5)$ | (1,0,0,10,0,0) |
| $S_2(3,6,12)$ | $J(12,6)$ | (1,0,0,20,0,0,1) |
| $S(5,6,12)$ | $J(12,6)$ | (1,0,45,40,45,0,1) |
| $S(4,7,23)$ | $J(23,7)$ | (1,0,0,0,140,0,112,0) |
| $S(5,8,24)$ | $J(24,8)$ | (1,0,0,0,280,0,448,0,30) |
| 汉明(7) | $H(7,2)$ | (1,0,0,7,7,0,0,1) |
| X-汉明(7) | $H(8,2)$ | (1,0,0,0,14,0,0,0,1) |
| 二元戈莱 | $H(23,2)$ | (1,0,0,0,0,0,0,253,506,0,0,1288,…) |
| X-二元戈莱 | $H(24,2)$ | (1,0,0,0,0,0,0,0,759,0,0,0,2576,0,…) |
| 三元戈莱 | $H(11,3)$ | (1,0,0,0,0,132,132,0,330,110,0,24) |
| *-三元戈莱 | $H(11,3)$ | (1,0,0,0,0,0,132,0,0,110,0,0) |

**定理 30.3** 一个结合方案的非空子集的分布向量 $a$ 满足

$$\boldsymbol{a}Q \geqslant \boldsymbol{0},$$

这里 $\boldsymbol{0}$ 是 $k+1$ 个零的行向量.

**证明** 设 $\phi \in \mathbb{R}^X$ 是 $Y$ 的特征向量，这就是

$$\phi(x) = \begin{cases} 1 & \text{如果 } x \in Y, \\ 0 & \text{如果 } x \notin Y. \end{cases}$$

则

$$a_i = \frac{1}{|Y|}\phi A_i \phi^{\top}.$$

因为 $E_\ell$ 是幂等的且对称的，

$$\begin{aligned} 0 \leqslant \|\phi E_\ell\|^2 &= (\phi E_\ell)(\phi E_\ell)^{\top} = \phi E_\ell \phi^{\top} \\ &= \frac{1}{N}\phi\left(\sum_{i=0}^{k} Q_\ell(i) A_i\right)\phi^{\top} = \frac{|Y|}{N}\sum_{i=0}^{k} Q_\ell(i) a_i. \end{aligned}$$

■

417

我们进一步注意到，第 $\ell$ 个不等式中的等号成立当且仅当射影 $\phi E_\ell$ 是零向量．第 0 个不等式是平凡的，因为 $\boldsymbol{a}Q$ 的第 0 个坐标是 $a_0+a_1+\cdots+a_k$，这当然是非负的.

**例 30.8** 对 $J(8,3)$，当分数约去后 Delsarte 不等式是

$$15 + 7a_1 - a_2 - 9a_3 \geqslant 0,$$
$$30 + 2a_1 - 5a_2 + 9a_3 \geqslant 0,$$
$$10 - 2a_1 + a_2 - a_3 \geqslant 0.$$

这些不等式可视为有给定分布向量$(1, a_1, a_2, a_3)$的一个 8-集合的 3-子集的族 $\mathcal{F}$ 存在的必要

条件.

当假定某个 $a_i$ 为零时，我们可以问它们关于 $|\mathcal{F}|$ 蕴涵着什么. 例如，假设$a_3=0$($\mathcal{F}$ 中没有两个成员是不相交的). $1+a_1+a_2(=|\mathcal{F}|)$在满足这些不等式的条件下的最大值是 21，这是一个线性规划问题. 根据埃德斯-柯召-拉多定理，即定理 6.4，我们已经知道 $|\mathcal{F}|\leqslant 21$. 定理 30.3 蕴涵定理 6.4，见本章的评注.

定理 30.3 导致关于码的基数的线性规划界. 对汉明方案 $H(n, q)$，给定一个整数 $d$，我们可以考虑线性规划问题

"在 $a_i\geqslant 0$ 和$(1, 0, \cdots, 0, a_d, a_{d+1}, \cdots, a_n)Q\geqslant\mathbf{0}$ 的条件下最大化 $1+a_d+a_{d+1}+\cdots+a_n$"，这里 $Q$ 是该方案的$(n+1)\times(n+1)$第二个特征矩阵. 如果 LPB 表示 $1+a_d+a_{d+1}+\cdots+a_n$ 在这些条件下的最大值，且 $C$ 是最小距离至少为 $d$ 的长度为 $n$ 的任意 $q$ 元码，因为 $C$ 的分布向量 $\boldsymbol{a}$ 满足这些条件且坐标之和为 $|C|$，因此 $|C|\leqslant$LPB.

对汉明方案我们提到，如果 $\boldsymbol{a}$ 是一个线性码 $C$ 的分布向量，则 $\frac{1}{|C|}\boldsymbol{a}Q$ 是其对偶码 $C^{\perp}$ 的分布向量. 为了明白这一点，只需把 MacWilliams 定理(即定理 20.3)中的公式与定理 30.1(ii)中的公式加以比较. 这无疑解释了对一个线性码的分布向量 $\boldsymbol{a}$，为何 $\boldsymbol{a}Q\geqslant\mathbf{0}$，但我们上面已经证明，即使 $C$ 不是线性的，它仍然成立.

一般地，很难从线性规划界(LPB)提取有用的信息，但可以证明它至少比球装填界(SPB，即定理 21.1)好；见 Delsarte(1973). 对小的参数值，可以利用单纯形算法显式地计算这个界. 在二元码的情形，对一些 $n$ 和 $d$ 的值我们已经这样做了，结果显示在图 30.2 的表中. 该表给出一个非负向量$(1, 0, \cdots, 0, a_d, a_{d+1}, \cdots, a_n)$，其和在满足 $\boldsymbol{a}Q\geqslant\mathbf{0}$ 的条件下最大. 对于读者，尝试确定表中给出的满足 LPB 的码是否真实存在是个不错的练习. 我们提及从称为 Nordstrom-Robinson 码的一个长度为 16 的有趣二元码可以得到几个码，该码有 256 个码字且最小距离为 6. 它不是线性的. 见问题 30I 和问题 30J.

| $n$ | $d$ | SPB | LPB | $a_0$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | $a_6$ | $a_7$ | $a_8$ | $a_9$ | $a_{10}$ | $a_{11}$ | $a_{12}$ | $a_{13}$ | $a_{14}$ | $a_{15}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 3 | 170.7 | 170.7 | 1 | 0 | 0 | 18.3 | 36.7 | 29.3 | 29.3 | 36.7 | 18.3 | 0 | 0 | 1 | | | | |
| 11 | 5 | 30.6 | 24 | 1 | 0 | 0 | 0 | 0 | 11 | 11 | 0 | 0 | 0 | 0 | 1 | | | | |
| 11 | 7 | 8.8 | 4 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | | | | |
| 12 | 3 | 315.1 | 292.6 | 1 | 0 | 0 | 20 | 45 | 48 | 56 | 65.1 | 40.7 | 11.4 | 3.4 | 1.7 | 0.1 | | | |
| 12 | 5 | 51.9 | 40 | 1 | 0 | 0 | 0 | 0 | 15 | 17.5 | 0 | 0 | 5 | 1.5 | 0 | 0 | | | |
| 12 | 7 | 13.7 | 5.3 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2.7 | 1.7 | 0 | 0 | 0 | 0 | | | |
| 13 | 3 | 585.1 | 512 | 1 | 0 | 0 | 22 | 55 | 72 | 96 | 116 | 87 | 40 | 16 | 6 | 1 | 0 | | |
| 13 | 5 | 89.0 | 64 | 1 | 0 | 0 | 0 | 0 | 18 | 24 | 4 | 3 | 10 | 4 | 0 | 0 | 0 | | |
| 13 | 7 | 21.7 | 8 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 3 | 0 | 0 | 0 | 0 | 0 | | |
| 14 | 3 | 1092.3 | 1024 | 1 | 0 | 0 | 28 | 77 | 112 | 168 | 232 | 203 | 112 | 56 | 28 | 7 | 0 | 0 | |
| 14 | 5 | 154.6 | 128 | 1 | 0 | 0 | 0 | 0 | 28 | 42 | 8 | 7 | 28 | 14 | 0 | 0 | 0 | 0 | |
| 14 | 7 | 34.9 | 16 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | 7 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 15 | 3 | 2048 | 2048 | 1 | 0 | 0 | 35 | 105 | 168 | 280 | 435 | 435 | 280 | 168 | 105 | 35 | 0 | 0 | 1 |
| 15 | 5 | 270.8 | 256 | 1 | 0 | 0 | 0 | 0 | 42 | 70 | 15 | 15 | 70 | 42 | 0 | 0 | 0 | 0 | 1 |
| 15 | 7 | 56.9 | 32 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 15 | 15 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

图 30.2

418 ~ 419

Bose-Mesner 代数的两组基之间，以及 Bose-Mesner 代数上的普通乘法和阿达马乘法之间似乎有一种"对偶性"．有时会发生这种情况：存在第二个结合方案使得后者的 $E_i$ 在阿达马乘法之下的行为与前者的 $A_i$ 在普通乘法(标量因子除外)下的行为相似，且反之亦然．当两个方案中一个的第一个特征矩阵 $P$ 等于另一个的第二个特征矩阵 $Q$ 时，说这两个方案是形式对偶的(参见下面的问题 30E)．已知许多对形式对偶的强正则图．如上面提到的汉明方案，它与自身是形式对偶的．约翰逊方案通常没有形式对偶，因为一般来说它的克赖因参数不是整数，克赖因参数的定义如下．

一个结合方案的克赖因参数是由

$$NE_i \circ E_j = \sum_{\ell=0}^{k} q_{ij}^{\ell} E_\ell \tag{30.7}$$

定义的 $(k+1)^3$ 个数 $q_{ij}^{\ell}$．如果该方案有形式对偶，则这些数是形式对偶的参数 $p_{ij}^{\ell}$ 且因此为非负整数．我们总有

$$q_{ij}^{\ell} \geqslant 0, \quad \text{对所有} \quad 0 \leqslant i,j,\ell \leqslant k,$$

因为 $q_{ij}^{\ell}$ 是两个半正定矩阵的阿达马积的特征值，因此是非负的，参见问题 21E．原则上，克赖因参数是原始参数 $p_{ij}^{\ell}$ 的函数(见问题 30E)且它们的非负性可以视为有给定参数的方案存在的必要条件；在定理 21.3 中我们对强正则图做了这件事．

**问题 30E** 对一个给定特征矩阵 $Q$ 的方案，怎样计算其参数 $q_{ij}^{\ell}$？也就是说，证明它们由 $Q$ 唯一确定．

后面我们需要知道

$$q_{ii}^{0} = m_i, \quad q_{ij}^{0} = 0, \quad \text{对} \quad i \neq j. \tag{30.8}$$

420

当考虑(30.7)两端矩阵的所有项时，得出左端的项之和是 $N$ 乘以

$$\langle E_i, E_j \rangle = \begin{cases} m_i & \text{如果 } i = j, \\ 0 & \text{其他}. \end{cases}$$

对码和设计的一些应用，我们需要知道更多有关方案的知识．然而在考虑特殊方案之前，我们可以针对一般的方案证明一个有趣的结果．

给定一个 $k$-类方案和 $\{1, 2, \cdots, k\}$ 的一个子集 $K$，对方案的点集的一个子集 $Y$，当每一对不同的元素 $x$, $y \in Y$，对某个 $j \in K$，$x$ 和 $y$ 是第 $j$ 次结合时，$Y$ 称为 $K$-团．当没有一对元素 $x$, $y \in Y$ 对任意 $j \in K$ 是第 $j$ 次结合时，称 $Y$ 是 $K$-余团．如果 $G$ 是邻接矩阵为 $\sum_{j \in K} A_j$ 的图，则 $G$ 中的团与方案中的 $K$-团相同，且 $G$ 中的余团(点的独立集)与方案中的 $K$-余团相同．

**定理 30.4** *在集合 $\mathfrak{X}$ 上的一个 $k$-类结合方案中，设 $A \subseteq \mathfrak{X}$ 是一个 $K$-余团且 $B \subseteq \mathfrak{X}$ 是一个 $K$-团，这里 $K \subseteq \{1, 2, \cdots, k\}$，则*

$$|A||B| \leqslant N.$$

**证明** 设 $\boldsymbol{a} = (a_0, a_1, \cdots, a_k)$ 是 $A$ 的分布向量且 $\boldsymbol{b} = (b_0, b_1, \cdots, b_k)$ 是 $B$ 的分布向量．

在定理 30.2 的第一个方程中取逆，前面乘以 $\boldsymbol{a}$ 且后面乘以 $\boldsymbol{b}^{\top}$ 得

$$\boldsymbol{a}Q\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & m_1 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & 0 & \cdots & m_k\end{bmatrix}^{-1}(\boldsymbol{b}Q)^{\top}=N\boldsymbol{a}\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & n_1 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & 0 & \cdots & n_k\end{bmatrix}^{-1}\boldsymbol{b}^{\top}. \tag{30.9}$$

由定理 30.3，$\boldsymbol{a}Q$ 和 $\boldsymbol{b}Q$ 都是非负向量. 它们的第 0 个坐标分别是 $|A|$ 和 $|B|$，因此(30.9)左边的标量至少是 $|A|\ |B|$. 我们的假设蕴涵对 $i>0$，$a_ib_i=0$，所以(30.9)右端的标量是 $N$. ■

定理 30.4 中等号成立的例子是 $S(t,\ k,\ v)$存在时的 $J(v,\ k)$. 取 $K=\{1,\ 2,\ \cdots,\ k-t\}$. 则 $S(t,\ k,\ v)$的区组集是一个 $K$-余团. 包含一个固定的 $t$-子集的所有 $k$-子集的集合是一个 $K$-团. 定理 30.4 中等号成立的例子是存在完全 $e$-纠错码 $C$ 时的 $H(n,\ q)$. 取$K=\{1,\ 2,\ \cdots,\ 2e\}$，则 $C$ 是一个 $K$-余团. 围绕一个固定字、半径为 $e$ 的球是一个 $K$-团. 421

**问题 30F** 找出一个例子使 $|A|\ |B|>|G|$ 成立，这里 $G$ 是一个正则图，$A$ 是它的团，$B$ 是它的余团.

**问题 30G** 如果图 $G$ 有一个自同构的迁移群，$A$ 是 $G$ 的团且 $B$ 是 $G$ 的余团，证明 $|A|\ |B|\leqslant|G|$.

下面定义*多项式方案*，其中有两种类型. 一个结合方案(其结合矩阵有特定的编号 $A_1$，$A_2$，…，$A_k$)称为 *$P$-多项式的*，如果对 $i=0,\ 1,\ 2,\ \cdots,\ k$，$A_i$ 在 $A_1$ 中是一个次数为 $i$ 的多项式. 一个结合方案(其幂等元有特定的编号 $E_1$，$E_2$，…，$E_k$)称为 *$Q$-多项式的*，如果对 $i=0,\ 1,\ \cdots,\ k$，$E_i$ 在 $E_1$ 中是一个次数为 $i$ 的阿达马多项式(我们指存在一个 $i$ 次多项式使得通过应用该多项式于 $E_1$ 的每个项得到 $E_i$).

**问题 30H** 证明一个结合方案是 $P$-多项式的，当且仅当它是一个度量方案.

$Q$-多项式方案也称为*余度量的*，但对此似乎没有简单的几何解释. 我们使用术语“度量的”和“余度量的”，而不用“$P$-多项式的”和“$Q$-多项式的”.

可以看出汉明方案和约翰逊方案是余度量的，见 Delstarte(1973).

在一个度量方案中，定义一个 *$d$-码*是子集 $S\subseteq\mathfrak{X}$，$S$ 的特征向量 $\phi$ 满足

$$\phi A_i\phi^{\top}=0,\quad 对\ i=1,2,\cdots,d-1.$$

在一个余度量方案中，定义一个 *$t$-设计*是子集 $S\subseteq\mathfrak{X}$，$S$ 的特征向量 $\phi$ 满足

$$\phi E_i\phi^{\top}=0,\quad 对\ i=1,2,\cdots,t.$$

$d$-码的组合意义是直截了当的：$S$ 是一个 $d$-码，当且仅当对 $i<d$，$S$ 中没有两个不同的元素是第 $i$ 次结合. 因此，在汉明方案中，$S$ 是一个$(2e+1)$-码，当且仅当它是一个 $e$-纠错码，即最小距离至少为 $2e+1$. $t$-设计的组合意义不是太明显，只有对特定的方案有更多的了解才能理解其组合意义. 注意 $S$ 是一个 $t$-设计当且仅当定理 30.3 中关于 $S$ 的分布向量的前 $t$ 个非平凡的不等式中的等号成立，即对 $i=1,\ \cdots,\ t$，$\phi E_i=\mathbf{0}$. 422

下面的定理解释了在约翰逊方案和汉明方案中的设计，它们分别与 $t$-设计和正交阵列的经典概念对应. 在有 $q$ 个符号的集合 $A$ 上，指标为 $\lambda$ 且强度为 $t$ 的*正交阵列*是 $\lambda q^t$ 个字的 $A^n$ 的一

个子集 $C$，使得对 $n$ 个坐标中 $t$ 个的每一选择，$A$ 中元素的每个可能的 $t$ 元组恰在 $C$ 的成员的那些坐标($t$ 个)中出现 $\lambda$ 次.

**定理 30.5** (i)一个 $v$-集合的 $k$-子集的族 $S$ 作为 $J(v, k)$的一个子集考虑时是一个 $t$-设计，当且仅当它在经典的意义下是一个 $t$-设计的区组的集合.

(ii)来自 $q$ 个元素的一张字母表 $A$ 的 $n$ 元组的一个族 $S$ 作为 $H(n, q)$的一个子集考虑时是一个 $t$-设计，当且仅当它是一个强度为 $t$ 的正交阵列的列集.

**部分证明** 我们将证明这两个方案中 $t$-设计的定义蕴涵集族 $S$ 是一个经典的 $t$-设计或正交阵列，(i)和(ii)的逆的证明留给读者.

在结合方案的意义下，设 $S$ 在 $J(v, k)$中是一个 $t$-设计且 $\phi$ 为其特征向量. 在例 30.7 中，看到 $E_0+E_1+\cdots+E_t$ 是到一个空间上的正交射影，当 $T$ 遍历 $v$-空间的 $t$-子空间时这个空间由 $\boldsymbol{e}_T$ 生成. $S$ 的成员包含一个 $t$-子集 $T$，这些成员的数目是

$$\phi\boldsymbol{e}_T^{\top}=\phi(E_0+E_1+\cdots+E_t)\boldsymbol{e}_T^{\top}=\phi E_0\boldsymbol{e}_T^{\top}.$$

因为 $E_0$ 是全幺矩阵 $J$ 的一个标量倍，这个数目与特定的 $t$-子集 $T$ 无关.

423 在结合方案的意义下，设 $S$ 在 $H(n, q)$中是一个 $t$-设计且 $\phi$ 是其特征向量. 在例 30.6 中，描述了 $q=2$ 时的特征空间，我们仅在这一情形证明本定理. 完整的证明可在 Delsarte(1973)中找到.

用例 30.6 中的记号，

$$\langle\phi,\boldsymbol{v}_a\rangle=\sum_{b\in S}(-1)^{\langle a,b\rangle},$$

因此 $S$ 是一个 $t$-设计当且仅当

$$\text{对重量}\leqslant t\text{的所有非零}a,\qquad \sum_{b\in S}(-1)^{\langle a,b\rangle}=0.$$

例如，当 $a$ 的重量取为 1 时，上面的等式蕴涵在任意给定的坐标位置，$S$ 的一半成员有项 0，一半成员有项 1. 当 $a$ 的重量取为 2 时，例如 $a$ 取(1，1，0，0，…，0)，等式蕴涵 $S$ 中以 00 或 11 开始的成员数等于以 10 或 01 开始的成员数；由此及上面的叙述得出，在 $S$ 中恰有 1/4 的 $n$ 元组以 00，10，01 和 11 开始.

一般地，考虑坐标位置的一个 $t$-子集 $T\subseteq\{1, 2, \cdots, n\}$. 对 $T$ 的每个子集 $I$，设 $\lambda_I$ 表示在 $I$ 的坐标中项为 1 且在 $T\setminus I$ 的坐标中项为 0 的 $a\in S$ 的数目. 对 $T$ 的每个子集 $J$，设 $a_J$ 表示在 $J$ 的坐标中为 1 且在其余的 $n-|J|$ 个坐标中为 0 的二元 $n$-数组. 我们有 $2^t$ 个线性方程，对每个 $J\subseteq T$ 有一个：

$$\sum_{|I\cap J|\equiv 0(\mathrm{mod}\ 2)}\lambda_I-\sum_{|I\cap J|\equiv 1(\mathrm{mod}\ 2)}\lambda_I=\begin{cases}|S| & \text{如果 } J=\varnothing\\ 0 & \text{其他.}\end{cases}$$

显然，对所有的 $I\subseteq T$，$\lambda_I=|S|/2^t$ 是这个方程组的一组解. 这个方程组的系数矩阵是 $2^t$ 阶阿达马矩阵(见第 18 章)，特别地，它是非奇异的，因此解是唯一的. 于是 $S$ 是一个强度为 $t$ 的正交阵列. ■

接下来的两个定理是“形式对偶的”. 也就是说，它们的证明是类似的，但 $A_i$ 和 $E_i$ 的基的

角色互换了，如矩阵的普通乘法和阿达马乘法. 对于汉明方案，定理 30.6(i)化为球装填界，即定理 21.1，且(iii)对等号成立(完全码——见第 20 章)给出了一个非常强的条件，属于 S. P. Lloyd(1957). 对于约翰逊方案，定理 30.7(i)化为定理 19.8，且(iii)对等号成立(紧设计——见第 19 章)给出了一个非常强的条件，属于 Ray-Chaudhuri and Wilson(1975). [424]

**定理 30.6** 设 $C$ 为集合 $\mathfrak{X}$ 上的一个 $k$-类度量结合方案中的$(2e+1)$-码. 设 $\phi\in\mathbb{R}^{\mathfrak{X}}$是 $C$ 的特征向量.

(i)我们有

$$|C|\leqslant N/(1+n_1+n_2+\cdots+n_e).$$

(ii)至少存在 $e$ 个下标 $i\in\{1,2,\cdots,k\}$使得

$$\phi E_i\phi^{\top}\neq 0.$$

(iii)在(i)中等号成立当且仅当在(ii)中等号成立，在这种情况下 $e$ 个使得 $\phi E_i\phi^{\top}\neq 0$ 的下标 $i$ 正好是使

$$\sum_{\ell=0}^{e}P_\ell(i)=0$$

的整数 $i$.

**证明** 设 $\phi$ 为$(2e+1)$-码 $C$ 的特征向量并考虑表达式

$$\alpha:=\phi(c_0A_0+c_1A_1+\cdots+c_eA_e)^2\phi^{\top},$$

这里 $c_0$，$c_1$，…，$c_e$ 是标量. 我们用两种方式计算 $\alpha$.

引入

$$f(i):=c_0P_0(i)+c_1P_1(i)+\cdots+c_eP_e(i)$$

作为 $c_j$ 的一个函数. 由(30.3)，$c_0A_0+c_1A_1+\cdots+c_eA_e=\sum_{i=0}^{k}f(i)E_i$，因此

$$\alpha=\left(\sum_{i=0}^{k}f(i)\phi E_i\right)\left(\sum_{i=0}^{k}f(i)\phi E_i\right)^{\top}=\sum_{i=0}^{k}f(i)^2\phi E_i\phi^{\top}.$$

[425]

另一方面，$A_i$ 是 $A_1$ 中一个次数为 $i$ 的多项式，于是$(A_0+A_1+\cdots+A_e)^2$ 是 $A_1$ 中一个次数为 $2e$ 的多项式，因此它是 $A_0$，$A_1$，…，$A_{2e}$的一个线性组合. 我们的假设蕴涵对 $i=1,2,\cdots,2e$，$\phi A_i\phi^{\top}=0$. 因此，为计算 $\alpha$，当$(A_0+A_1+\cdots+A_e)^2$ 写成 $A_0$，$A_1$，…，$A_{2e}$的线性组合时，我们仅需知道 $A_0$ 的系数；由(30.2)和(30.1)，

$$\alpha=\left(\sum_{i,j=0}^{e}c_ic_jp_{ij}^0\right)\phi A_0\phi^{\top}=\left(\sum_{i=0}^{e}c_i^2n_i\right)|C|.$$

注意，由(30.6)，$f(0)=c_0n_0+c_1n_1+\cdots+c_en_e$. 现在我们结合 $\alpha$ 的两个值，记住 $E_0=\frac{1}{N}J$，因此 $\phi E_0\phi^{\top}=\frac{1}{N}|C|^2$，目的是得到

$$(c_0^2+c_1^2n_1+\cdots+c_e^2n_e)|C|=\sum_{i=0}^{k}f(i)^2\phi E_i\phi^{\top}$$

$$\geqslant \frac{1}{N}(c_0 + c_1 n_1 + \cdots + c_e n_e)^2 \mid C \mid^2. \tag{30.10}$$

从(30.10)可以得到定理的每一部分. 当取 $c_i := 1$ 时得到(i).

为证明(ii), 作相反的假设, 存在少于 $e$ 个下标 $i \geqslant 1$ 使得 $\phi E_i \phi^\top \neq 0$. 由初等线性代数, 存在不全为零的标量 $c_0$, $c_1$, …, $c_e$, 使得对 $i=0$ 和所有使 $\phi E_i \phi^\top \neq 0$ 的 $i$ 有 $f(i)=0$. 那么(30.10)给出 $\mid C \mid \sum_{i=0}^{e} n_i c_i^2 = 0$, 矛盾.

假设(i)中等号成立. 那么在所有 $c_i$ 等于 1 时, (30.10)表明对 $e$ 个或更多个使 $\phi E_i \phi^\top \neq 0$ 的 $i$ 值, $f(i) = \sum_{\ell=0}^{e} P_\ell(i) = 0$. 我们断言 $f(i)=0$ 不能对超过 $e$ 个 $i$ 值成立. 这是因为 $f(0)$, $f(1)$, …, $f(k)$是 $A_0 + A_1 + \cdots + A_e$ 的特征值, $A_0 + A_1 + \cdots + A_e$ 是 $A_1$ 中一个次数为 $e$ 的多项式; 这就是, $f(0)$, …, $f(k)$来自在 $A_1$ 的特征值 $P_1(0)$, …, $P_1(k)$上计算一个 $e$ 次的多项式. (矩阵 $A_1$ 有 $k+1$ 个不同的特征值, 因为它产生一个 $k+1$ 维的代数.)我们的断言由一个 $e$ 次多项式至多有 $e$ 个零点得出. 因此(ii)在这种情况下等号成立且(iii)被证明.

426

最终, 假设在(ii)中等号成立. 选择标量 $c_0$, …, $c_e$ 使得对所有使 $\phi E_i \phi^\top \neq 0$ 的 $i$ 有 $f(i) = 0$ 且 $f(0) = 1$. 则(30.10)给出 $\mid C \mid = N(c_0^2 + c_1^2 n_1 + \cdots + c_e^2 n_e)$. 柯西-施瓦茨(Cauchy-Schwartz)不等式证明

$$1 = \left(\sum_{i=0}^{e} c_i n_i\right)^2 \leqslant \left(\sum_{i=0}^{e} c_i^2 n_i\right)\left(\sum_{i=0}^{e} n_i\right),$$

因此 $\mid C \mid \geqslant N/(1 + n_1 + n_2 + \cdots + n_e)$. 于是(i)中的等号成立. ■

**推论**(Lloyd 定理) *如果规模为 $q$ 的字母表上存在长度为 $n$ 的一个完全 $e$-纠错码, 则*

$$L_e(x) := \sum_{i=0}^{e} (-1)^i \binom{n-x}{e-i} \binom{x-1}{i} (q-1)^{e-i}$$

*有 $e$ 个不同的整数零点.*

**证明** 这正是定理 30.6(iii)对汉明方案的陈述. 和 $\sum_{\ell=0}^{e} P_\ell(x)$化简为上述的 $L_e(x)$, 这里 $P_\ell(x)$与定理 30.1(ii)中的相同. ■

**例 30.9** 我们证明不存在非平凡的二元完全 2-纠错码. 如果这样一个码的长度 $n > 2$, 则其基数是 $2^n \Big/ \left(1 + n + \binom{n}{2}\right)$, 因此对某个整数 $r$, $1 + n + \binom{n}{2} = 2^r$. (有这种性质的 $n$ 是反常的——但可能发生, 如 $n = 90$ 时.)由定理 30.1(ii), 对 $H(n, 2)$,

$$P_0(x) + P_1(x) + P_2(x) = 2x^2 - 2(n+1)x + 1 + n + \binom{n}{2},$$

那么定理 30.6(iii)断言

$$x^2 - (n+1)x + 2^{r-1} = 0$$

有两个整数根 $x_1$ 和 $x_2$. 我们一定有 $x_1 = 2^a$ 且 $x_2 = 2^b$, 这里 $a$, $b$ 为正整数, $a + b = r - 1$ 且 $2^a + 2^b = n + 1$. 容易验证

$$(2^{a+1}+2^{b+1}-1)^2=2^{a+b+4}-7.$$ [427]

如果 $a$ 和 $b$ 都大于等于 2，则上式左边$\equiv 1(\mathrm{mod}\ 16)$，同时右边$\equiv 9(\mathrm{mod}\ 16)$，矛盾．读者应考虑其他情形，将会发现唯一的可能是$\{a, b\}=\{1, 2\}$，在这一情形 $n=5$.

**定理 30.7** 设 $D$ 是集合 $\mathscr{X}$ 上的一个 $k$-类余度量结合方案中的 $2s$-设计．设 $\phi\in\mathbb{R}^{\mathscr{X}}$ 为 $D$ 的特征向量．

(i)我们有

$$|D|\geqslant 1+m_1+m_2+\cdots+m_s.$$

(ii)至少有 $s$ 个下标 $i\in\{1, 2, \cdots, k\}$使得

$$\phi A_i\phi^{\top}\neq 0.$$

(iii)(i)中的等号成立当且仅当(ii)中的等号成立，在这一情形使得 $\phi A_i\phi^{\top}\neq 0$ 的 $s$ 个下标 $i$ 恰是使

$$\sum_{\ell=0}^{s}Q_\ell(i)=0$$

的那些整数 $i$.

**证明** 设 $\phi$ 为一个 $2s$-设计 $D$ 的特征向量并考虑表达式

$$\beta:=\phi(c_0E_0+c_1E_1+\cdots+c_sE_s)\circ(c_0E_0+c_1E_1+\cdots+c_sE_s)\phi^{\top},$$

这里 $c_0, c_1, \cdots, c_s$ 是标量．我们用两种方式计算 $\beta$.

引入

$$g(i):=\frac{1}{N}(c_0Q_0(i)+c_1Q_1(i)+\cdots+c_sQ_s(i))$$

作为 $c_i$ 的一个函数．由(30.4)，$c_0E_0+c_1E_1+\cdots+c_sE_s=\sum_{i=0}^{k}g(i)A_i$，因此

$$\beta=\left(\sum_{i=0}^{k}g(i)\phi A_i\right)\circ\left(\sum_{i=0}^{k}g(i)\phi A_i\right)^{\top}=\sum_{i=0}^{k}g(i)^2\phi A_i\phi^{\top}.$$ [428]

另一方面，在 $E_1$ 中 $E_i$ 是一个次数为 $i$ 的阿达马多项式，因此 $E_0+E_1+\cdots+E_s$ 的阿达马平方在 $E_1$ 中是一个次数为 $2s$ 的阿达马多项式，于是是 $E_0, E_1, \cdots, E_{2s}$的一个线性组合．我们的假设蕴涵对 $i=1, 2, \cdots, 2s$，$\phi E_i\phi^{\top}=0$. 因此当 $E_0+E_1+\cdots+E_s$ 的阿达马平方写成 $E_0$，$E_1, \cdots, E_{2s}$的线性组合时，我们仅需知道 $E_0$ 的系数；由(30.7)和(30.8)，

$$\beta=\left(\frac{1}{N}\sum_{i,j=0}^{s}c_ic_jq_{ij}^{0}\right)\phi E_0\phi^{\top}=\frac{1}{N^2}\left(\sum_{i=0}^{s}c_i^2m_i\right)|C|^2.$$

注意，由(30.6)，$g(0)=\frac{1}{N}(c_0m_0+c_1m_1+\cdots+c_sm_s)$. 现在我们结合 $\beta$ 的两个值，得到

$$\frac{1}{N^2}(c_0^2+c_1^2m_1+\cdots+c_s^2m_s)|C|^2=\sum_{i=0}^{k}g(i)^2\phi A_i\phi^{\top}$$

$$\geqslant \frac{1}{N}(c_0 + c_1 m_1 + \cdots + c_s m_s)^2 \mid C \mid. \qquad (30.11)$$

以与定理 30.6 的证明类似的方式从(30.11)得出定理的每一部分. ■

**问题 30I** 考虑扩展的戈莱码 $G_{24}$. 为了记号的方便，排列坐标使得字 $\boldsymbol{c}=(1, \cdots 1, 0, \cdots, 0)$是一个码字，$\boldsymbol{c}$ 的前 8 个位置是 1，在其余的位置上是 0.

(i)利用计数论证来证明 $G_{24}$包含重量为 8 的 30 个字，这些字在前 8 个位置没有 1(因此到 $\boldsymbol{c}$ 的距离是 16). 然后证明 $G_{24}$中没有 1 在前 8 个位置的所有字组成一个子码，该子码在本质上是 $R(1, 4)$.

(ii)设 $A$ 是 $G_{24}$ 里从字 $\boldsymbol{a}=(a_1, a_2, \cdots, a_{24})$中去掉前 8 个坐标得到的 16 元组$(a_9, a_{10}, \cdots, a_{24})$的一个集合，但 $\boldsymbol{a}$ 满足$(a_1, a_2, \cdots, a_7)$的重量$\leqslant 1$. 证明 $A$ 是有 256 个码字且最小距离为 6 的长度为 16 的码.

429 (iii)利用 $A$ 构造几个码的例子，其中等号在图 30.2 中成立.

**问题 30J** 证明参数为[13, 6, 5]的二元线性码不存在.（因此也不存在参数为[16, 8, 6]的二元线性码.）

**问题 30K** 奇图以一个$(2k+1)$-集合的$k$-子集作为顶点，如果两个 $k$-子集不相交，它们由一条边相连.（对 $k=2$，这是彼得森图.）

(i)证明这个图是距离正则的.

(ii)证明：如果 $k=3$，与费诺平面“对应的”顶点在该图上形成一个完全码.

**问题 30L** 在约翰逊方案 $J(v, 3)$中找出完全 3-码的所有例子.（所有的例子都是平凡的.）

## 评注

结合方案由统计学家与部分平衡设计同时引入. 一个关联结构相对于其点上的一个结合方案是部分平衡的，如果第 $i$ 次结合的每对出现在常数 $\lambda_i$ 个区组中. 例子包括第 21 章中的部分几何. 引入部分平衡设计是为了避开费希尔不等式 $b\geqslant v$，或等价地 $r\geqslant k$，这对部分平衡设计不必成立. 重复实验花费金钱($r$ 代表“重复次数”)或占用时间，因此由于实践上的原因，人们希望 $r$ 较小.

为了进行实验分析，在该实验中使用了一定的设计(关联结构)，必须计算 $NN^{\top}$，这里 $N$ 是关联矩阵，这些计算在部分平衡设计中大为简化，这是因为在一个 $m$-类方案中，

$$NN^{\top} = \lambda_0 A_0 + \lambda_1 A_1 + \cdots + \lambda_m A_m$$

位于小维数的 Bose-Mesner 代数中，即使矩阵的规模可能比方案的维数 $m+1$ 大得多.

Delsarte 不等式蕴涵一般的埃德斯-拉多定理：如果 $n\geqslant(t+1)(k-t+1)$且$\mathcal{F}$是一个 $n$-集合的 $k$-子集的族，$\mathcal{F}$ 的任意两个成员相交于至少 $t$ 个点，则 $|\mathcal{F}|\leqslant\binom{n-t}{k-t}$. 见 Wilson

430 (1984a).

关于完全码的不存在性的更多内容，见 Van Lint(1999).

## 参考文献


E. Bannai and T. Ito (1984), *Association Schemes*, Benjamin/Cummings.

A. E. Brouwer, A. M. Cohen, and A. Neumaier (1989), *Distance Regular Graphs*, Springer-Verlag.

Ph. Delsarte (1973), *An Algebraic Approach to the Association Schemes of Coding Theory*, Philips Res. Rep. Suppl. **10**.

Ph. Delsarte (1975), The association schemes of coding theory, in: *Combinatorics* (Proc. Nijenrode Conf.), M. Hall, Jr. and J. H. van Lint, eds., D. Reidel.

J. H. van Lint (1999), *Introduction to Coding Theory*, Third edition, Springer-Verlag.

S. P. Lloyd (1957), Binary block coding, *Bell System Tech. J.* **36**, 517–535.

D. K. Ray-Chaudhuri and R. M. Wilson (1975), On $t$-designs, *Osaka J. Math.* **12**, 737–744.

R. M. Wilson (1984a), The exact bound in the Erdős-Ko-Rado theorem, *Combinatorica* **4**, 247–257.

R. M. Wilson (1984b), On the theory of $t$-designs, pp. 19–50 in: *Enumeration and Design* (Proceedings of the Waterloo Silver Jubilee Conference), D. M. Jackson and S. A. Vanstone, eds., Academic Press.


431

# 第31章 图论中(更多)的代数技术

在第9章我们对图的邻接矩阵使用线性代数技术，在第21章更是广泛应用．在这里我们汇集一些其他的巧妙应用．也见第36章．

竞赛图是完全图的一个定向，也就是说，对任意两个不同的顶点 $x$ 和 $y$，边或者从 $x$ 到 $y$，或者从 $y$ 到 $x$，但不能既从 $x$ 到 $y$ 又从 $y$ 到 $x$ 的有向图．竞赛图在问题3D中简要地引入．一个有向图的邻接矩阵当从 $x$ 到 $y$ 有一条边时，在位置$(x, y)$上有一个1，否则为0．

**引理 31.1** *$n$ 个顶点上的一个竞赛图的邻接矩阵 $A$ 的秩为 $n$ 或者 $n-1$.*

**证明** 竞赛图的定义保证 $A+A^{\top}=J-I$，这里所有的矩阵都是 $n\times n$ 阶的．假设 $A$ 的秩至多为 $n-2$．则存在一个非零的向量 $\boldsymbol{x}$ 使得 $\boldsymbol{x}A=0$ 且 $\boldsymbol{x}J=0$，我们接着计算

$$0=\boldsymbol{x}(A+A^{\top})\boldsymbol{x}^{\top}=\boldsymbol{x}(J-I)\boldsymbol{x}^{\top}=-\boldsymbol{x}\boldsymbol{x}^{\top}<0,$$

这与 $\boldsymbol{x}$ 的存在性矛盾． ■

下面的定理属于 R. L. Graham 和 H. O. Pollak，他们的原始证明应用了 Sylvester 定律，他们也把该定理用于定理9.1的证明中．



**定理 31.2** *假设完全图 $K_n$ 可以表示为 $k$ 个边不交的子图 $H_1$，$H_2$，…，$H_k$ 的并，这里每个 $H_i$ 是一个完全二部图．则 $k\geqslant n-1$.*

**证明** 通过从两个颜色类中的一类到另一类的所有边指定一个方向给每个完全二部子图 $H_i$ 定向．这产生 $n$ 个顶点的一个竞赛图，其邻接矩阵 $A$ 是 $k$ 个有向图 $H_i$ 的邻接矩阵 $A_i$(通过包括所有的顶点扩大为 $n\times n$ 矩阵)的和．这样一个完全有向二部子图的邻接矩阵，经过给顶点的适当地重新编号，有块形式

$$\begin{bmatrix} O & J & O \\ O & O & O \\ O & O & O \end{bmatrix},$$

特别地，其秩为1．这蕴涵着 $A$ 的秩至多为 $k$，根据引理31.1，完成本定理的证明． ■

这使我们想起德布鲁因-埃德斯定理，即定理19.1，该定理以完全不同的术语断言，如果 $K_n$ 是边不交的 $k$ 个完全子图的并，则 $k\geqslant n$．定理19.1的证明也完全不同．但尚不知道不用线性代数如何证明定理31.2.

作为一个实对称矩阵，一个有限图 $G$ 的邻接矩阵 $A=A(G)$ 有特征向量的一组正交基．(对应于不同特征值的特征向量必然是正交的.)“$G$ 的特征值”是指 $A(G)$ 的特征值．下面是一张谱的表，即一些图的全部特征值的列表：

| 图 | 谱 |
|---|---|
| $K_5$ | 4，−1，−1，−1，−1 |
| $K_{3,3}$ | 3，0，0，0，0，−3 |
| 立方体 | 3，1，1，1，−1，−1，−1，−3 |
| 五边形 | 2，$\frac{1}{2}(-1+\sqrt{5})$，$\frac{1}{2}(-1+\sqrt{5})$，$\frac{1}{2}(-1-\sqrt{5})$，$\frac{1}{2}(-1-\sqrt{5})$ |

(续)

| 图 | 谱 |
|---|---|
| 彼得森图 | 3, 1, 1, 1, 1, 1, −2, −2, −2, −2 |
| $L_2(3)$ | 4, 1, 1, 1, 1, −2, −2, −2, −2 |
| Heawood 图 | 3, $\sqrt{2}$, $\sqrt{2}$, $\sqrt{2}$, $\sqrt{2}$, $\sqrt{2}$, $\sqrt{2}$, $-\sqrt{2}$, $-\sqrt{2}$, $-\sqrt{2}$, $-\sqrt{2}$, $-\sqrt{2}$, $-\sqrt{2}$, −3 |

433

(Heawood 图是费诺构形的“二部邻接图”，七个顶点代表点且另外的七个顶点代表线. 该图在第 35 章会再次出现.)

不同构的图可以有相同的谱. 例如，在第 21 章我们提到存在四个不同构的强正则图，它们有 $T(8)$的参数，参见定理 21.5.

**问题 31A** 证明在 $K_{10}$中不可能找到三个边不交的彼得森图的拷贝. 提示：如果 $A_1$，$A_2$ 和 $A_3$ 是 $K_{10}$的三个边不交的彼得森子图的邻接矩阵，则三个矩阵有相同的谱，它们都有一个全 1 的向量 $\boldsymbol{j}$ 作为特征向量，且 $A_1+A_2+A_3=J-I$.

设 $S$ 为一个对称矩阵，对 $\boldsymbol{x}\neq\boldsymbol{0}$，表达式 $\boldsymbol{x}S\boldsymbol{x}^\top/\boldsymbol{x}\boldsymbol{x}^\top$ 称为瑞利(Raleigh)商. 设 $\boldsymbol{e}_1$，$\boldsymbol{e}_2$，…，$\boldsymbol{e}_n$ 是对应的特征值

$$\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_n$$

的特征向量的一组正交基. 如果我们把 $\boldsymbol{x}$ 由这组基写出，比如说 $\boldsymbol{x}=a_1\boldsymbol{e}_1+\cdots+a_n\boldsymbol{e}_n$，则

$$\frac{\boldsymbol{x}S\boldsymbol{x}^\top}{\boldsymbol{x}\boldsymbol{x}^\top}=\frac{\lambda_1a_1^2+\lambda_2a_2^2+\cdots+\lambda_na_n^2}{a_1^2+a_2^2+\cdots+a_n^2}. \tag{31.1}$$

特别地，对任意非零的 $\boldsymbol{x}$，

$$\lambda_1\geqslant\frac{\boldsymbol{x}S\boldsymbol{x}^\top}{\boldsymbol{x}\boldsymbol{x}^\top}\geqslant\lambda_n.$$

虽然我们要考虑的大多数图是简单图，但这并不妨碍考虑下面的多重图的邻接矩阵(这里在 $x$ 行和 $y$ 列的项是连结 $x$ 和 $y$ 的边的数目)，或“赋权”图的邻接矩阵(这里在 $x$ 行和 $y$ 列的项是与连结 $x$ 和 $y$ 的边相联系的“重量”).

首先令人惊奇的是，一个图的谱与图的更加几何化或组合化的性质密切相关. 最早观察到的联系之一是下面的 A. J. Hoffman 定理. 在图 $G$ 中，一个余团或顶点的一个独立集，是顶点的一个集合，其中没有两个顶点是相邻的.

434

**定理 31.3** 设 $G$ 是有 $n$ 个顶点的 $d$ 度正则图，又设 $\lambda_{\min}$是 $G$ 的最小特征值，于是 $\lambda_{\min}$是负的. 则对 $G$ 中的任意一个余团 $S$，

$$|S|\leqslant\frac{-n\lambda_{\min}}{d-\lambda_{\min}}.$$

**证明** 设 $A$ 是$G$ 的邻接矩阵且$\lambda:=\lambda_{\min}$. 则 $A-\lambda I$ 是半正定的，即所有的特征值都是非负的；注意 $A-\lambda I$ 的特征向量与 $A$ 的特征向量相同，特征向量之一是 $\boldsymbol{j}:=(1,1,\cdots,1)$，我们有

$$j(A-\lambda I)=(d-\lambda)j.$$

则对

$$M:=A-\lambda I-\frac{d-\lambda}{n}J,$$

我们得到 $jM=0$. $A$ 的每个其他的特征向量 $e$ 可取作与 $j$ 正交，因此 $eJ=0$，可以看出 $e$ 也是有非负特征值的 $M$ 的一个特征向量. 也就是说，$M$ 也是半正定的.

现在设 $\phi$ 是由 $G$ 的 $m$ 个顶点组成的一个余团 $S$ 的特征向量，即如果 $x\in S$，则 $\phi(x)$ 等于 1，否则 $\phi(x)$ 等于 0. 那么 $\phi A\phi^{\top}=0$ 且我们有

$$0\leqslant \phi M\phi^{\top}=-\lambda\phi\phi^{\top}-\frac{d-\lambda}{n}\phi J\phi^{\top}=-\lambda m-\frac{d-\lambda}{n}m^2.$$

从而得出定理中所陈述的不等式. ■

对非正则图，关于定理 31.3 有许多推广和变化——见 Haemers(1979).

**问题 31B** 把定理 31.3 应用到一个简单正则图 $G$ 的补，目的是根据谱得到 $G$ 中团的规模的一个上界. 找出一些例子满足你得到的界.

**问题 31C** 一个简单图 $G$ 的线图 $L=L(G)$ 已在第 17 章引入. 例如，在第 21 章定义的 [435] $L_2(m)$ 是 $K_{m,m}$ 的线图，$T(m)$ 是 $K_m$ 的线图，且一个五边形的线图还是五边形. (i)证明彼得森图不是任何一个图的线图. (ii)证明：如果 $G$ 的边比顶点多，则线图 $L(G)$ 的最小特征值是 $-2$. (提示：设 $N$ 是 $G$ 的邻接矩阵并考虑 $N^{\top}N$.)

L. Lovász(1979) 观察到，定理 31.3 中关于余团的规模的界也是所谓的图的香农(Shannon)容量的界. 这是源自信息论的一个概念. 假设“字母”的一个集合被用于传送信息. 有些字母对被假定为“易混淆的”. 我们说两个潜在的消息(字或这些字母的长为 $n$ 的串)是易混淆的，如果这些字母的每个坐标或者是相同的，或者是易混淆的. 我们希望得到字的一个集合，其中没有两个字是易混淆的.

为了对此用更加图论化的术语加以叙述，我们引入一个图 $G$，其顶点是字，两个顶点是相邻的当且仅当这两个字是易混淆的. 因此字的一个集合，其中没有两个是易混淆的，恰是这个图中的一个余团. 简单图 $G$ 和 $H$ 的*强积* $G\otimes H$ 是由 $V(G\otimes H):=V(G)\times V(H)$ 定义的简单图，这里当 $x_1$ 和 $x_2$ 相等或相邻，$y_1$ 和 $y_2$ 相等或相邻时，不同的点 $(x_1, y_1)$ 和 $(x_2, y_2)$ 相邻. $G^n:=G\otimes G\otimes\cdots\otimes G$($n$ 个因子)的顶点对应长度为 $n$ 的字，且在 $G^n$ 中两个字相邻仅当它们是易混淆的. 因此我们对 $G^n$ 中最大余团的规模感兴趣.

一个图 $G$ 的*独立数* $\alpha(G)$ 是 $G$ 中余团的最大基数. 图 $G$ 的*香农容量*是

$$\Theta(G):=\lim_{n\to\infty}(\alpha(G^n))^{1/n}=\sup_n(\alpha(G^n))^{1/n}.$$

该极限存在且等于 $(\alpha(G^n))^{1/n}$ 的上确界，这由观察 $G$ 和 $H$ 中余团的积是 $G\otimes H$ 的余团，以及 $\alpha(G^{k+m})\geqslant\alpha(G^k)\alpha(G^m)$ 得出. (见第 11 章中的 Fekete 引理.)

[436] **例 31.1** 在相关的代数技巧被 Lovász 注意到之前，像计算五边形 $P_5$ 这样的简单图的香农容量问题多年未得到解决. 容易找到长度为 $n$ 的 $2^n$ 个字，其中没有两个是易混淆的，例如，全由 1 和 3 组成的所有的字. 这证明 $\Theta(P_5)\geqslant 2$. 这个界并不那么好，不难发现五个字的一个

集合

$$(1,1),(2,3),(3,5),(4,2),(5,4),$$

我们仅得到长度为 2 的四个字. 对偶数的 $n$ 值，为得到长度为 $n$ 的$(\sqrt{5})^n$ 个两两不易混淆的字，可以取上面五个字的 $n/2$ 个拷贝的积，这证明 $\Theta(P_5)\geqslant\sqrt{5}$. 对非常大的 $n$ 值，我们能做得更好吗? 不是的，在定理 31.6 之后我们会看到 $\Theta(P_5)\leqslant\sqrt{5}$.

这里是 Lovász(1979)的思路. 首先，观察到用第 18 章中克罗内克积的定义，对向量 $\boldsymbol{x}$, $\boldsymbol{y}\in\mathbb{R}^n$, $\boldsymbol{v}$, $\boldsymbol{w}\in\mathbb{R}^n$, 我们有

$$(\boldsymbol{x}\circ\boldsymbol{v})(\boldsymbol{y}\circ\boldsymbol{w})^{\mathrm{T}}=\langle\boldsymbol{x},\boldsymbol{y}\rangle\langle\boldsymbol{v},\boldsymbol{w}\rangle. \tag{31.2}$$

设 $G$ 为一个图. 为了简单起见，我们总假设其顶点是 1, 2, …, $n$. $G$ 的规范正交表示是在欧几里得空间中的一组单位向量($\boldsymbol{v}_1$, …, $\boldsymbol{v}_n$)，使得如果 $i$ 和 $j$ 是不相邻的顶点，则$\boldsymbol{v}_i$ 和$\boldsymbol{v}_j$ 是正交的. 显然，每个图都有规范正交表示，例如由两两正交的向量得到的图.

**引理 31.4** *设($\boldsymbol{u}_1$, …, $\boldsymbol{u}_n$)和($\boldsymbol{v}_1$, …, $\boldsymbol{v}_m$)分别是 $G$ 和 $H$ 的规范正交表示. 则向量 $\boldsymbol{u}_i\circ\boldsymbol{v}_j$ 构成$G\otimes H$ 的规范正交表示.*

**证明** 这是(31.2)的一个结论.

定义一个规范正交表示($\boldsymbol{u}_1$, …, $\boldsymbol{u}_n$)的值是

$$\min_{c}\max_{1\leqslant i\leqslant n}\frac{1}{\langle\boldsymbol{c},\boldsymbol{u}_i\rangle^2},$$

这里 $\boldsymbol{c}$ 遍历所有的单位向量，产生最小值的向量 $\boldsymbol{c}$ 称为该表示的*柄*. 设 $\theta(G)$表示 $G$ 的所有表示上的最小值. 容易看出这个最小值可以达到. 具有值 $\theta(G)$的表示称为*最优的*. ■ 437

**引理 31.5** $\theta(G\otimes H)\leqslant\theta(G)\theta(H)$.

**证明** 设($\boldsymbol{u}_1$, …, $\boldsymbol{u}_n$)和($\boldsymbol{v}_1$, …, $\boldsymbol{v}_m$)分别是 $G$ 和 $H$ 的最优规范正交表示，它们具有柄 $\boldsymbol{c}$ 和 $\boldsymbol{d}$，则由(31.2)，$\boldsymbol{c}\circ\boldsymbol{d}$ 是一个单位向量，又由(31.2)，

$$\begin{aligned}\theta(G\otimes H)&\leqslant\max_{i,j}\frac{1}{\langle\boldsymbol{c}\circ\boldsymbol{d},\boldsymbol{u}_i\circ\boldsymbol{v}_j\rangle^2}\\&=\max_{i,j}\frac{1}{\langle\boldsymbol{c},\boldsymbol{u}_i\rangle^2}\circ\frac{1}{\langle\boldsymbol{d},\boldsymbol{v}_j\rangle^2}\\&=\theta(G)\theta(H).\end{aligned}$$

(可以证明在这个引理中等号成立.) ■

**定理 31.6** $\Theta(G)\leqslant\theta(G)$.

**证明** 我们先证 $\alpha(G)\leqslant\theta(G)$. 设($\boldsymbol{u}_1$, …, $\boldsymbol{u}_n$)是 $G$ 的最优规范正交表示，该表示具有柄 $\boldsymbol{c}$. 假设在 $G$ 中{1, 2…, $k$}是最大独立集，因此 $\boldsymbol{u}_1$, …, $\boldsymbol{u}_k$ 是两两正交的. 所以

$$1=\|\boldsymbol{c}\|^2\geqslant\sum_{i=1}^{k}\langle\boldsymbol{c},\boldsymbol{u}_i\rangle^2\geqslant\alpha(G)/\theta(G).$$

由这个式子和引理 31.5 可以得到 $\alpha(G^n)\leqslant\theta(G^n)\leqslant\theta(G)^n$. ■

**例 31.1**(续) 由来自 Lovász(1979)的一个好主意，现在我们能证明 $\Theta(G_5)=\sqrt{5}$. 考虑一把其柄和五根伞骨都是单位长度的伞. 如果我们撑开这样一把伞，会经过一个点，在那里不相

邻的伞骨之间的角都是 $\pi/2$. 如果称柄为 $\boldsymbol{c}$ 且伞骨为从 $\boldsymbol{u}_1$ 到 $\boldsymbol{u}_5$，方向是离它们的公共点而去，则 $\boldsymbol{u}_1$，…，$\boldsymbol{u}_5$ 是$\mathbb{R}^3$ 中 $C_5$ 的一个正交表示. 证明$\langle \boldsymbol{c}, \boldsymbol{u}_i\rangle = 5^{-1/4}$是一项容易的计算. 由定理 31.6 和 $\theta(5)$的定义给出结果.

这个结果也可以从下面的推论得出.

**推论 31.7** 设 $G$ 是 $n$ 个顶点上的 $d$ 度正则图，又设 $\lambda_{\min}$是 $G$ 的最小特征值，则

438

$$\Theta(G) \leqslant \frac{-n\lambda_{\min}}{d-\lambda_{\min}}.$$

**证明** 设 $A$ 是 $G$ 的邻接矩阵. 在定理 31.3 的证明中我们看到对 $\lambda := \lambda_{\min}$，$M := A - \lambda I - \frac{d-\lambda}{n}J$ 是半正定(且奇异)的. 因此对某个秩$<n$ 的实矩阵 $B$，$M = BB^{\top}$. 设 $B$ 的行为 $\boldsymbol{x}_1$，…，$\boldsymbol{x}_n$，我们有

$$\langle \boldsymbol{x}_i, \boldsymbol{x}_i\rangle = -\lambda - \frac{d-\lambda}{n}, \quad \langle \boldsymbol{x}_i, \boldsymbol{x}_j\rangle = -\frac{d-\lambda}{n},$$

后者当 $i$，$j$ 不相邻时成立. 设 $\boldsymbol{c}$ 是任意一个与 $B$ 的行 $\boldsymbol{x}_i$ 正交的单位向量，并定义

$$\boldsymbol{v}_i := \frac{1}{\sqrt{-\lambda}}\boldsymbol{x}_i + \frac{1}{\sqrt{-\lambda n/(d-\lambda)}}\boldsymbol{c}.$$

检验$\boldsymbol{v}_1$，…，$\boldsymbol{v}_n$ 是 $G$ 的一个正交表示. 最终注意到，对任意 $i$，

$$\frac{1}{\langle \boldsymbol{c}, \boldsymbol{v}_i\rangle^2} = \frac{-\lambda n}{d-\lambda}.$$

推论的结果由定理 31.6 得到. ■

接下来，我们给出特征值“交错”的两个应用.

**引理 31.8** 设 $A$ 为特征值是

$$\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$$

的 $n$ 阶对称矩阵. 假设 $N$ 是使得 $NN^{\top} = I_m$ 的 $m \times n$ 实矩阵，因此 $m<n$. 设 $B := NAN^{\top}$，又设

$$\mu_1 \geqslant \mu_2 \geqslant \cdots \geqslant \mu_m$$

为 $B$ 的特征值. 则在

$$\lambda_i \geqslant \mu_i \geqslant \lambda_{n-m+i}$$

的意义下，$B$ 的特征值在 $A$ 的特征值中交错，其中 $i=1, 2, \cdots, m$.

**证明** 设 $\boldsymbol{e}_1$，…，$\boldsymbol{e}_n$ 是 $A$ 的对应于$\lambda_1$，…，$\lambda_n$ 的特征向量的一组正交基，$\boldsymbol{f}_1$，…，$\boldsymbol{f}_m$ 是 $B$ 的对应于$\mu_1$，…，$\mu_m$ 的特征向量的一组正交基.

439

固定 $i$ 并考虑 $U := \operatorname{span}\{\boldsymbol{f}_1, \cdots, \boldsymbol{f}_i\}$. 由(31.1)，对每个非零的 $\boldsymbol{x} \in U$，

$$\frac{\boldsymbol{x}B\boldsymbol{x}^{\top}}{\boldsymbol{x}\boldsymbol{x}^{\top}} \geqslant \mu_i.$$

设 $W := \{\boldsymbol{x}N : \boldsymbol{x} \in U\}$. 则 $W$ 是一个 $i$ 维子空间且对每个 $\boldsymbol{y} \in W$，

$$\frac{\boldsymbol{y}A\boldsymbol{y}^{\top}}{\boldsymbol{y}\boldsymbol{y}^{\top}} \geqslant \mu_i. \tag{31.3}$$

在 $W\cap\mathrm{span}\{\boldsymbol{e}_i, \boldsymbol{e}_{i+1}, \cdots, \boldsymbol{e}_n\}$ 中选择 $\boldsymbol{y}\neq 0$，则除(31.3)外，从(31.1)我们有

$$\frac{\boldsymbol{y}A\boldsymbol{y}^{\top}}{\boldsymbol{y}\boldsymbol{y}^{\top}}\leqslant\lambda_i,$$

这证明了 $\lambda_i\geqslant\mu_i$.

用 $U:=\mathrm{span}\{\boldsymbol{f}_i, \cdots, \boldsymbol{f}_m\}$，类似的论证可证明 $\mu_i\geqslant\lambda_{n-m+i}$. ■

在 $m=n-1$ 时，项的交错似乎是最自然的，这里

$$\lambda_1\geqslant\mu_1\geqslant\lambda_2\geqslant\mu_2\geqslant\lambda_3\geqslant\cdots\geqslant\lambda_{n-1}\geqslant\mu_{n-1}\geqslant\lambda_n.$$

引理 31.8 的一个重要特殊情形是，$N$ 的行是长度为 $n$ 的 $m$ 个不同的"标准基"向量，即每行有单独一个 1. 在这一情形，$B$ 是 $A$ 的一个 $m\times m$ 阶主子矩阵. 下面的观察属于 D. M. Cvetković.

**定理 31.9** 一个图 $G$ 中，余团的规模不能超过 $G$ 的非负特征值的数目，或 $G$ 的非正特征值的数目.

**证明** 如果 $G$ 有规模为 $m$ 的一个余团，则 $G$ 的邻接矩阵 $A$ 有一个全零的 $m\times m$ 主子矩阵. 如果 $A$ 的特征值是 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_n$，则由交错，$\lambda_m\geqslant 0$ 且 $0\geqslant\lambda_{n-m+1}$，因此 $A$ 至少有 $m$ 个特征值 $\geqslant 0$ 且至少有 $m$ 个特征值 $\leqslant 0$. ■

下一个定理是 A. J. Hoffman 关于图的色数的一个结果. 我们说对正则图，这个定理可由定理 31.3 得出. [440]

**定理 31.10** 设 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_n$ 是一个图 $G$ 的特征值，则

$$\chi(G)\geqslant 1+\lambda_1/(-\lambda_n).$$

**证明** 设 $G$ 能用 $m$ 种颜色正常地染色，颜色类导出 $G$ 的邻接矩阵的一个划分

$$A=\begin{bmatrix}A_{11} & \cdots & A_{1m}\\ \vdots & & \vdots\\ A_{m1} & \cdots & A_{mm}\end{bmatrix},$$

这里 $A_{ij}$ 是行由颜色 $i$ 的顶点指示且列由颜色 $j$ 的顶点指示的子矩阵. 每个对角块 $A_{ii}$ 是一个项为零的方阵.

设 $\boldsymbol{e}$ 是 $A$ 的一个特征向量，它与最大的特征值 $\lambda_1$ 对应，并写成 $\boldsymbol{e}=(\boldsymbol{e}_1, \cdots, \boldsymbol{e}_m)$，这里 $\boldsymbol{e}_i$ 的坐标被颜色为 $i$ 的顶点指示. 设

$$N:=\begin{bmatrix}\frac{1}{\|\boldsymbol{e}_1\|}\boldsymbol{e}_1 & 0 & 0 & \cdots\\ 0 & \frac{1}{\|\boldsymbol{e}_2\|}\boldsymbol{e}_2 & 0 & \cdots\\ 0 & 0 & \frac{1}{\|\boldsymbol{e}_3\|}\boldsymbol{e}_3 & \cdots\\ \vdots & \vdots & \vdots & \cdots\end{bmatrix}$$

(一个 $m\times n$ 矩阵)并设 $B:=NAN^{\top}$. 由引理 31.8，$B$ 的特征值 $\mu_1, \cdots, \mu_m$ 与 $A$ 的特征值交

错，因此在 $\lambda_1$ 与 $\lambda_n$ 之间. 另一方面，我们已构造的 $B$ 使得 $\lambda_1$ 是其一个特征值，这是因为

$$(\|e_1\|,\cdots,\|e_m\|)B = eAN^\top = \lambda_1 eN^\top = \lambda_1(\|e_1\|,\cdots,\|e_m\|).$$

最后，注意 $B$ 的对角项为零，因此

$$0 = \mathrm{trace}(B) = \mu_1 + \cdots + \mu_m \geqslant \lambda_1 + (m-1)\lambda_n.$$

441 这就证明了定理.（也许我们应该说 $e_i$ 中的某个为零，这些行不包括在 $N$ 中.） ■

**问题 31D** 证明：对任意一个有限图 $G$，$\chi(G)\leqslant 1+\lambda_1$，这里 $\lambda_1$ 为 $G$ 的最大特征值. 提示：考虑 $G$ 的一个诱导子图的度，该子图相对于与 $G$ 有相同的色数的子图是最小的.

除对称之外，一个图 $G$ 的邻接矩阵也是非负矩阵. 这样的矩阵有一个有用的理论，其中心是佩龙-弗罗贝尼乌斯定理，即下面的定理 31.11. 完整的证明见 Gantmacher(1959).

比如说，行和列由一个集合 $X$ 指示的方阵 $A$ 称为不可约的，如果不可能找到 $X$ 的一个真子集 $S$ 使得只要 $x\in S$ 且 $y\in X\setminus S$，就有 $A(x, y)=0$. 等价地，$A$ 不是不可约的，当且仅当有可能由同时的行置换和列置换得到一个形如

$$\begin{bmatrix} B & O \\ C & D \end{bmatrix}$$

的矩阵，这里 $B$ 和 $D$ 是阶至少为 1 的方阵. 很显然，如果 $A$ 是一个图的邻接矩阵，则它不可约当且仅当 $G$ 是连通的.

**问题 31E** 设 $D$ 是一个有限的有向图，$A$ 是 $D$ 的邻接矩阵，或行和列由 $D$ 的顶点指示的任何一个矩阵，这里如果没有边从 $x$ 指向 $y$，则 $A(x, y)=0$；如果有这样的边，则 $A(x, y)>0$. (i)证明 $A^k(x, y)>0$ 当且仅当在 $D$ 中从 $x$ 到 $y$ 有一条长度为 $k$ 的有向步路. (ii)证明 $A$ 是不可约的当且仅当 $D$ 是强连通的，即当且仅当对 $D$ 中的任意两个顶点 $x$，$y$，从 $x$ 到 $y$ 有一条有向路.

**定理 31.11**（佩龙-弗罗贝尼乌斯） *设 $A$ 为一个 $n\times n$ 的不可约非负矩阵. 不计倍数，存在一个唯一的特征向量 $\boldsymbol{a}=(a_1, \cdots, a_n)$，其所有坐标 $a_i$ 都是非负的. 事实上，这个向量 $\boldsymbol{a}$ 的坐标是正的.* 442 *对应的特征值 $\lambda$（称为 $A$ 的控制特征值）有代数重数 1 且对 $A$ 的任意一个特征值 $\mu$ 有 $\lambda\geqslant|\mu|$.*

**部分证明** 我们略去非负特征向量的存在性的证明，但说明不可约性如何被利用并给出余下的大部分证明.

首先证明，$A$ 的与特征值 $\lambda$ 对应的任何一个非负特征向量，比如说 $\boldsymbol{a}$，在所有的坐标上是正的. 如问题 31E 中那样把 $A$ 作为一个强连通有向图的矩阵考虑. 因为从任意一个顶点到另外一个顶点的有向路的长度$\leqslant n-1$，

$$I + A + A^2 + \cdots + A^{n-1} > O.$$

在这里和下面，将关于矩阵或向量的不等式理解为对所有的坐标成立. 因为 $\boldsymbol{a}\geqslant\mathbf{0}$ 但 $\boldsymbol{a}\neq\mathbf{0}$，

$$\mathbf{0} < \boldsymbol{a}(I + A + A^2 + \cdots + A^{n-1}) = (1 + \lambda + \cdots + \lambda^{n-1})\boldsymbol{a},$$

因此 $\mathbf{0}<\boldsymbol{a}$.

接下来证明特征值 $\lambda$ 有几何重数 1，即它对应的特征空间的维数为 1. 设 $\boldsymbol{a}'$ 是与特征值 $\lambda$ 对应的任意一个特征向量，坐标是正的、负的或零. 如果从 $\boldsymbol{a}$ 中加或减去 $\boldsymbol{a}'$ 的一个小的标量

倍，我们得到另一个正的或非负的特征向量$\boldsymbol{a}-c\boldsymbol{a}'$与特征值$\lambda$对应. 可以选择$c$使得$\boldsymbol{a}-c\boldsymbol{a}'\geqslant\mathbf{0}$，但使$\boldsymbol{a}-c\boldsymbol{a}'$至少有一个坐标是零. 这与上面的结果矛盾，除非$\boldsymbol{a}-c\boldsymbol{a}'=\mathbf{0}$. 我们略去$\lambda$的代数重数为1，即$\lambda$是$A$的特征多项式的一个单零点的证明.

对$A$，设$\boldsymbol{a}$是对应特征值$\lambda$的正的特征向量. 设$\boldsymbol{b}$是$A^\top$的正的特征向量，比如说$A\boldsymbol{b}^\top=\nu\boldsymbol{b}^\top$. 则

$$\lambda\boldsymbol{a}\boldsymbol{b}^\top=(\boldsymbol{a}A)\boldsymbol{b}^\top=\boldsymbol{a}(A\boldsymbol{b}^\top)=\nu\boldsymbol{a}\boldsymbol{b}^\top.$$

这是一个矛盾，除非$\nu=\lambda$，因此$A\boldsymbol{b}^\top=\lambda\boldsymbol{b}^\top$. 假设$\boldsymbol{u}$是$A$的一个特征向量但不是$\boldsymbol{a}$的标量倍数，比如说满足$\mu\neq\lambda$的$\boldsymbol{u}A=\mu\boldsymbol{u}$. 则

$$\lambda\boldsymbol{u}\boldsymbol{b}^\top=\boldsymbol{u}(A\boldsymbol{b}^\top)=(\boldsymbol{u}A)\boldsymbol{b}^\top=\mu\boldsymbol{u}\boldsymbol{b}^\top.$$

443

这意味着$\boldsymbol{u}\boldsymbol{b}^\top=0$. 因此其他任意的特征向量$\boldsymbol{u}$不能有非负的坐标. 现在设$\hat{\boldsymbol{u}}:=(|u_1|,\cdots,|u_n|)$并检验$\hat{\boldsymbol{u}}A\geqslant|\mu|\hat{\boldsymbol{u}}$，这从$A\geqslant O$容易得出. 则

$$\lambda\hat{\boldsymbol{u}}\boldsymbol{b}^\top=\hat{\boldsymbol{u}}(A\boldsymbol{b}^\top)=(\hat{\boldsymbol{u}}A)\boldsymbol{b}^\top\geqslant|\mu|\hat{\boldsymbol{u}}\boldsymbol{b}^\top,$$

由此有$\lambda\geqslant|\mu|$. ■

**定理 31.12** *设$\lambda$是一个连通图$G$的控制特征值，则$G$是一个二部图当且仅当$-\lambda$也是$G$的一个特征值.*

**证明** 假设$G$是二部图，如果需要，顶点重新编号使得图的染色类由前$k$个顶点和后$n-k$个顶点组成，则$G$的邻接矩阵$A$有形式

$$A=\begin{bmatrix}O & B\\ B^\top & O\end{bmatrix},$$

这里$B$是$k\times(n-k)$矩阵. 设$\boldsymbol{e}$是与特征值$\mu$对应的一个特征向量并写成$\boldsymbol{e}=(\boldsymbol{e}_1,\boldsymbol{e}_2)$，这里$\boldsymbol{e}_1$由前$k$个坐标构成. 容易检验$(\boldsymbol{e}_1,-\boldsymbol{e}_2)$是特征值为$-\mu$的一个特征向量. 因此，如果$G$是一个二部图(连通的或不连通的)，其谱事实上是关于0对称的.

现在假设$\lambda$是一个连通图$G$的控制特征值且$-\lambda$也是一个特征值. 设$\boldsymbol{e}=(\boldsymbol{e}_1,-\boldsymbol{e}_2)$是对应于$-\lambda$的单位长度的一个特征向量，这里对顶点编号使得$\boldsymbol{e}_1$和$\boldsymbol{e}_2$都有非负的坐标. 相应地划分邻接矩阵$A$：

$$A=\begin{bmatrix}B & C\\ D & E\end{bmatrix}.$$

则

$$-\lambda=\boldsymbol{e}A\boldsymbol{e}^\top=\boldsymbol{e}_1B\boldsymbol{e}_1^\top+\boldsymbol{e}_2E\boldsymbol{e}_2^\top-\boldsymbol{e}_1C\boldsymbol{e}_2^\top-\boldsymbol{e}_2D\boldsymbol{e}_1^\top,$$

因此

$$(\boldsymbol{e}_1,\boldsymbol{e}_2)A(\boldsymbol{e}_1,\boldsymbol{e}_2)^\top\geqslant\lambda, \tag{31.4}$$

444

等号成立当且仅当

$$\boldsymbol{e}_1B\boldsymbol{e}_1^\top\overset{*}{=}\boldsymbol{e}_2E\boldsymbol{e}_2^\top=0. \tag{31.5}$$

等式(31.1)和$\lambda$是控制特征值的事实蕴涵在(31.4)中等号一定成立且$(\boldsymbol{e}_1,\boldsymbol{e}_2)$是对应于特征值

$\lambda$ 的一个特征向量. 那么定理 31.11 蕴涵$(\boldsymbol{e}_1, \boldsymbol{e}_2)$的所有坐标都是正的. 最终，(31.5)证明 $B=E=O$，这意味着 $G$ 是二部图. ■

**定理 31.13** 设 $G$ 是一个有限图且 $A$ 为其邻接矩阵，存在一个多项式 $f(x)$使得 $f(A)=J$ 当且仅当 $G$ 是连通且正则的.

**证明** 假设对某个多项式 $f(x)$，$f(A)=J$. 因为在一个给定矩阵中多项式是交换的，故 $AJ=JA$. $AJ$ 中在行 $x$ 和列 $y$ 的项是 $\deg_G(x)$. $JA$ 中在这个位置的项是 $\deg_G(y)$. 因此 $G$ 是正则的.

如果 $f(A)=J$，则特别地，对任意的 $x$ 和 $y$，对某个 $k$ 一定有 $A^k(x, y)\neq 0$. $A^k$ 中在行 $x$ 和列 $y$ 的项是 $G$ 中从 $x$ 到 $y$ 的长度为 $k$ 的步路的数目. 因此 $G$ 是连通的.

现在假设 $G$ 是连通且 $d$ 度正则的. 则 $\boldsymbol{j}$ 是 $A$ 的与特征值 $d$ 对应的一个特征向量. 根据定理 31.11，特征值 $d$ 有重数 1. 对任意的对称矩阵 $M$，到其特征空间上任何一个的正交射影的矩阵是 $M$ 的一个多项式；更明确一些，如果$(x-\mu_1)(x-\mu_2)\cdots(x-\mu_k)$是 $M$ 的极小多项式，证明

$$\frac{1}{(\mu_1-\mu_2)\cdots(\mu_1-\mu_k)}(M-\mu_2 I)\cdots(M-\mu_k I)$$

是到特征空间$\{\boldsymbol{a}:\boldsymbol{a}M=\mu_1\boldsymbol{a}\}$上的一个正交射影，这可作为一个练习. 因为到 $\boldsymbol{j}$ 的生成上的正交射影是$\frac{1}{v}J$，因此这个矩阵是 $A$ 的一个多项式. ■

同构的图有相同的特征值，但正如我们早先提到的，其逆不真：不同构的图可以有相同的谱(特征值的多重集). 见问题 21O. 但我们有部分的逆，尤其是对有素数个顶点的"循环图". [445]

设 $G$ 是一个写成加法的交换群. 对 $S\subseteq G$，凯莱图 $\Gamma(G, S)$有顶点集 $G$，且在$\Gamma(G, S)$中有一条从 $x$ 到 $y$ 的边，当且仅当 $y-x\in S$. 凯莱图在前面几章多次出现. 当$-S=S$时，一个凯莱图可以视为无向图；当 $0\notin S$ 时，凯莱图无环. 一个循环图是凯莱图 $\Gamma(G, S)$，其中 $G$ 是循环群.

(对非交换群也可以定义凯莱图，但下面我们只考虑交换群的情形.)

一个 $G$-矩阵是其行和列由 $G$ 的元素指示的方阵 $A$，这里对于对象的某个向量$(a_g: g\in G)$，有 $A(i, j)=a_{j-i}$. 一个循环矩阵(或简单地一个循环)是 $G$-矩阵，这里 $G$ 是循环的. 一般地，基于 $G$ 的一个凯莱图的邻接矩阵是 $G$-矩阵.

我们说一个环 $R$ 上的 $G$-矩阵在乘法之下封闭，且这样的矩阵的代数同构于第 28 章中出现的群环 $R[G]$.

**命题 31.14** 设 $\omega$ 是某个域 $F$ 中单位的 $n$ 次本原根且 $U$ 为其行和列由$\mathbb{Z}_n$指示的矩阵，这里 $U(i, j)=\omega^{ij}$. 设 $A$ 是基于 $F$ 的元素$(a_i: i\in\mathbb{Z}_n)$的一个循环，则 $UAU^{-1}$是对角项为

$$\lambda_j := \sum_{i=0}^{n-1} a_i\omega^{ji},\quad j=0,1,\cdots,n-1$$

的对角矩阵. 也就是说，$A$ 的特征值是 $\lambda_0$，$\lambda_1$，…，$\lambda_{n-1}$(且其对应的特征向量是 $U$ 的行).

**问题 31F** (i)证明命题 31.14. (ii)如果读者熟悉交换群的特征，证明当$\chi$遍历 $G$ 的特征时，一个有理的 $G$-矩阵 $A$ 的特征值是 $\lambda_\chi=\sum_{g\in G} a_g\chi(g)$，参见例 30.6.

如下的定理来自 Elspas and Turner(1970).

**定理 31.15** 设 $A$ 和 $B$ 是素数阶 $p>2$ 的有理循环矩阵，它们分别基于向量$(a_i: i\in\mathbb{Z}_p)$和$(b_i: i\in\mathbb{Z}_p)$. 如果 $A$ 和 $B$ 有相同的谱，则对$\mathbb{Z}_p$ 中的某个 $t\neq 0$，对所有的 $i\in\mathbb{Z}_p$，$a_i=b_{ti}$，这里下标模 $p$. [446]

**证明** 设 $\omega$ 为单位的一个 $p$ 次复本原根，则根据命题 31.14，$\alpha:=\sum_{i=0}^{n-1}a_i\omega^i$ 是 $A$ 的一个特征值，因此也是 $B$ 的特征值之一，于是对某个 $s$，

$$\sum_{i=0}^{n-1}a_i\omega^i=\sum_{i=0}^{n-1}b_i\omega^{si}.$$

首先假设 $s\neq 0$，并选择 $t$ 使得 $st\equiv 1(\mathrm{mod}\,p)$. 则

$$\sum_{i=0}^{p-1}(a_i-b_{ti})\omega^i=0.$$

但 $\omega$ 在有理数域上的最小多项式是 $1+x+x^2+\cdots+x^{p-1}$，因此可以得出结论：对某个常数 $c$，对所有的 $i$，$a_i-b_{ti}=c$. $A$ 和 $B$ 的迹分别为 $pa_0$ 和 $pb_0$，它们一定相等. 于是 $a_0=b_0$，故 $c=0$.

如果 $s=0$，则 $\alpha$ 为有理数且

$$(a_0-\alpha)+a_1\omega+\cdots+a_{p-1}\omega^{p-1}=0.$$

可以得出结论：上式的所有系数等于某个常数 $c$，这意味着 $A=\alpha T+cJ$.

$A$ 和 $B$ 的作用互换，重复以上的论证，发现或者定理的陈述成立，或者对某些有理数 $\beta$ 和 $d$，$B=\beta I+dJ$.

$aI+bJ$ 的特征值是重数为 1 的 $a+pb$ 和重数为 $p-1$ 的 $a+b$. 如果对 $p>2$，$A=\alpha I+cJ$ 和 $B=\beta I+dJ$ 有相同的谱，则 $A=B$ 且定理对任意 $t$ 成立. ■

我们说，对 $p=2$，定理的陈述不真，例如，循环行列式

$$\begin{bmatrix}1&1\\1&1\end{bmatrix}\quad 和 \quad\begin{bmatrix}1&-1\\-1&1\end{bmatrix}$$

有相同的谱$\{2,0\}$. 然而，当 $A$ 和 $B$ 都是非负时，定理为真. [447]

**推论** 素数阶的循环图是同构的当且仅当它们(它们的邻接矩阵)有相同的特征值.

**证明** 我们在前面已断言同构的图有相同的谱.

假设循环图 $\Gamma(\mathbb{Z}_p,S)$和 $\Gamma(\mathbb{Z}_p,T)$对 $S$，$T\subseteq\mathbb{Z}_p$ 有邻接矩阵 $A$ 和 $B$，其中 $p$ 为素数，$A$ 和 $B$ 的谱相同. 这里 $A$ 是基于$(a_i: i\in\mathbb{Z}_p)$的循环矩阵，如果 $i\in S$，$a_i=1$；否则 $a_i=0$. 类似地，$B$ 是基于$(b_i: i\in\mathbb{Z}_p)$的循环矩阵，如果 $i\in T$，$b_i=1$；否则 $b_i=0$. 定理 31.15 说(对 $p=2$，我们需要上面的附注)，对某个 $t\neq 0$，$a_i=b_{ti}$. $\mathbb{Z}_p$ 的置换 $\phi: i\to ti$ 是 $\Gamma(\mathbb{Z}_p,S)$到 $\Gamma(\mathbb{Z}_p,T)$上的一个同构，因为

$$i\to j,在\ \Gamma(\mathbb{Z}_p,S)\ 中 \Leftrightarrow i-j\in S$$
$$\Leftrightarrow t(i-j)\in T\Leftrightarrow ti\to tj\ ,在\ \Gamma(\mathbb{Z}_p,T)\ 中,$$

这里 $x\to y$ 意味着有一条边从 $x$ 指向 $y$. ■

**推论** 给定 $S$，$T\subseteq\mathbb{Z}_p$，循环图 $\Gamma(\mathbb{Z}_p, S)$ 和 $\Gamma(\mathbb{Z}_p, T)$ 是同构的，当且仅当对 $\mathbb{Z}_p$ 中的某个"乘子" $t\neq 0$，$T=tS$.

**证明** 如果 $\Gamma(\mathbb{Z}_p, S)$ 和 $\Gamma(\mathbb{Z}_p, T)$ 是同构的，则它们有相同的谱，如同在前一个引理的证明中，对某个 $t\neq 0$，我们有 $a_i=b_{ti}$，这意味着 $T=tS$.

反之，如果 $T=tS$，则如前面所介绍的，$\mathbb{Z}_p$ 的置换 $\phi: i\to ti$ 是一个同构. ■

曾经猜测：当 $p$ 由任意一个整数代替，条件 $t\neq 0$ 由 $(t, n)=1$ 代替时，这个推论成立，但对 $n=8$，9 及其他的值存在反例. 事实上，这个推论中的 $p$ 由 $n$ 代替时成立，如果 $n$ 恰好是无平方因子的数或 4 乘以一个无平方因子的奇数，见 M. Muzychuk(1997).

**问题 31G** 证明任意一个有限的简单图的顶点能被红色和蓝色染色，使得每个红色顶点与偶数个红色顶点相邻，且每个蓝色顶点与奇数个红色顶点相邻. 首先证明引理：如果 $S=(a_{ij})$ 是一个对称的(0，1)-矩阵，则对角线 $\boldsymbol{a}=(a_{11}, a_{22}, \cdots, a_{nn})$ 作为一个列向量考虑时，该向量位于域 $\mathbb{F}_2$ 上 $S$ 的列的生成中.

**问题 31H** 设 $G$ 是一个刚好有三个不同特征值的连通正则图，证明 $G$ 是强正则的.

**问题 31I** 设 $G$ 是一个非平凡的强正则图，对 $x\in V(G)$，设 $\Delta(x)$ 表示与 $x$ 不相邻的顶点导出的子图. (1)解释如果 $\Delta(x)$ 不连通，为何 $k-\mu$ 是 $G$ 的一个特征值，以及(2)通过计算证明 $k-\mu$ 不是 $G$ 的特征值. 通过(1)和(2)证明 $\Delta(x)$ 是连通的.

**问题 31J** 假设彼得森图 $P$ 是生成子图 $H$ 和 $K$ 的并，它们分别为 1 度和 2 度的正则图，设 $A$ 为 $P$ 的邻接矩阵且 $B$ 和 $C$ 是 $H$ 和 $K$ 的邻接矩阵，所以 $A=B+C$.

证明存在一个向量 $\boldsymbol{u}$ 是 $A$ 的对应于特征值 1 的特征向量，它也是 $B$ 的对应于特征值 $-1$ 的特征向量(因此是 $C$ 的对应于特征值 2 的特征向量). 其次，解释为何 $K$ 不能是一个连通图. (这证明 $P$ 不是一个哈密顿图.)

**问题 31K** 设 $G$ 是 $n$ 个顶点上的一个无重边的有向图，我们允许边 $a\to b$ 和 $b\to a$ 同时出现，在这种情形称边 $\{a, b\}$ 为一条无向边. 假设对任意两个顶点 $a$，$b$，如果 $a\neq b$，则恰有一条从 $a$ 到 $b$ 的长度为 3 的步路；如果 $a=b$，则没有这样的路径. 如果 $A$ 是 $G$ 的邻接矩阵，则这个性质由等式

$$A^3 = J - I \tag{31.6}$$

表示.

(i)证明 $G$ 是正则的.

(ii)如果 $c$ 是 $G$ 的度，证明 $n=c^3+1$.

(iii)证明 $G$ 恰有 $\frac{1}{2}(c^2+c)$ 条无向边.

(iv)如果 $n=9$，构造一个这样的图.

## 评注

定理 31.3 从来没有被 Hoffman(他是最早的"代数图论专家"之一)发表，但引起了许多听说过它的人的喜爱，因此成为经典.

问题 31D 是 H. Wilf 的一个结果，问题 31A 是 A. J. Schwenk 的一个未发表的结果.

## 参考文献


N. Biggs (1974), *Algebraic Graph Theory*, Cambridge University Press.

D. M. Cvetković, M. Doob, and H. Sachs (1979), *Spectra of Graphs, a Monograph*, V. E. B. Deutscher Verlag der Wissenschaften.

B. Elspas and J. Turner (1970), Graphs with circulant adjacency matrices, *J. Combinatorial Theory* **9**, 297–307.

F. R. Gantmacher (1959), *The Theory of Matrices*, Chelsea.

W. Haemers (1979), *Eigenvalue Techniques in Design and Graph Theory*, Mathematisch Centrum, Amsterdam.

L. Lovász (1979), On the Shannon capacity of a graph, *IEEE Trans. Information Theory* **25**, 1–7.

M. Muzychuk (1997), On Adam's conjecture for circulant graphs, *Discrete Math.* **176**, 285–298.


450

# 第 32 章　图的连通性

对 $k \geqslant 2$，称一个图 $G$ 是 *$k$-顶点连通的*，或者简单地说 *$k$-连通的*，当 $|V(G)| \geqslant k+1$ 时从 $G$ 中移去任意 $k-1$ 个顶点(以及关联的边)，得到的不是一个不连通的图，我们把"1-连通的"作为"连通的"同义词来用.

如果一个至少有 $k+1$ 个顶点的图 $G$ 不是 $k$-连通的，并且删去 $k-1$ 个顶点的集合 $S$ 使图不连通，则存在 $V(G) \setminus S$ 分成非空集合 $X$，$Y$ 的一个划分，使得没有边交叉(一个顶点在 $X$，另一个顶点在 $Y$). 设 $H$ 和 $K$ 是由 $X \cup S$ 和 $Y \cup S$ 导出的子图，但两端在 $S$ 中的边只放在 $H$ 或 $K$ 中的一个且只能是一个之中. 这样，我们得到边不交的子图 $H$ 和 $K$，它们的并是 $G$ 且使得 $|V(H) \cap V(K)| = k-1$. 反之，如果这样的 $H$ 和 $K$ 存在且每一个比它们的交至少多一个顶点，则 $G$ 不是 $k$-连通的.

若一个图是 2-连通的且没有环，就说它是 *不可分的*；若它是一个键图(两个顶点和任意正数条边连结它们，包括有一条这样的边的连杆图)、环图(一条边连结一个顶点自身)或者只有一个顶点的图，也说它是不可分的. 例如，所有的多边形都是不可分的；路图或其他至少有两条边的树不是不可分的.

(如果有其他边，我们不想要环，因为当删除关联的顶点时，在组合学的意义上可能没有使图不连通，但在拓扑学的意义上却使图不连通. 对塔特的 2-连通性的其他类型，不需要明确地禁止有环，或允许较小的图有环；参见问题 32D.)

451

下面是对不可分图的"结构"的一个初步观察.

**引理 32.1**　*设 $G$ 是一个至少有两条边的有限不可分图，且 $H$ 是 $G$ 的最大不可分的真子图，则 $G$ 是 $H$ 和连结 $H$ 的不同顶点且中间的顶点都不在 $H$ 中的路图 $P$ 的并.*

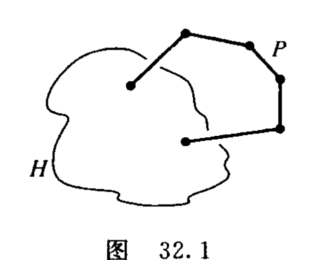



图　32.1

在以上引理的陈述中，路可称为"柄". 图 32.1 是一个例子.

**证明**　可能 $V(H)=V(G)$. 在这种情形，设 $e$ 是在 $G$ 中但不在 $H$ 中的一条边，并设 $P$ 是由 $e$ 和它的端点构成的连杆图. 因为添加 $e$ 到 $H$ 产生一个不可分的图且 $H$ 是不可分的真子图中的最大者，所以 $H$ 和 $P$ 的并是 $G$.

如果 $V(H) \neq V(G)$，$G$ 的连通性蕴涵存在一条边 $e$，它的一端 $x \in V(H)$ 且另一端 $y \notin V(H)$. 由 $G-x$ 的连通性，存在一条不经过 $x$ 的简单路连结 $y$ 和 $H$ 的某个其他顶点 $w$. 如果 $z$ 是在这条路上的 $H$ 的第一个顶点(当我们从 $y$ 前进到 $w$ 时)，边 $e$ 和这条路的原始部分提供了一个路图 $P$，$P$ 连结 $x$ 到 $z$，没有边在 $H$ 中且除了路的端点之外没有顶点在 $H$ 中. $H \cup P$ 是大于 $H$ 的不可分图，所以它等于 $G$. ■

作为这个引理的一个结论，给定至少有两条边的一个有限不可分图 $G$，存在不可分子图的一个序列：

$$H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_k = G,$$

这里 $H_0$ 是一个连杆图且每个 $H_{i+1}$ 是 $H_i$ 和一个柄的并.

图 $G$ 的细化的非正式定义是，由在一些边上插入额外的顶点而得到的图 $H$. 更精确一些，可以用(有限的)路图代替 $G$ 的边，这些路径内部的顶点是“新的”，即不是原始 $G$ 的顶点；而且允许用多边形代替环. 两个图被说成是同态的，如果它们同构于同一个图的细化. 不可分图(不是连杆图)的细化保持不可分性. 452

**问题 32A** 定义连通图 $G$ 的秩为 $|E(G)|-|V(G)|+1$. (在第 34 章，我们将会看到这是那里所说的 $G$ 的圈空间的维数.)当给一个不可分图增加一个柄时，秩增加 1. 秩为 0 的连通图是树. 秩为 1 的不可分图是多边形. 秩为 2 的不可分图是 $\theta$-图，它与字母 $\theta$ 同态，即有三条边的键图的细分，因为所有秩为 2 的不可分图可以由一个多边形添加一个柄得到. 四种图的细分描述秩为 3 的不可分图.

显然，如果 $G$ 不是不可分的，且 $H$，$K$ 是边不交的子图，它们至多有一个点是公共的，它们的并是 $G$，那么 $H$ 中的一条边和 $K$ 中的一条边不能都被 $G$ 的任何一个多边形包含.

**定理 32.2** *在一个不可分图 $G$ 中，任意两条边包含在一个多边形子图的边的集合中.*

**证明** 我们断定给定不可分图 $G$ 的不同顶点 $x$，$y$ 和一条边 $e$，存在一条从 $x$ 到 $y$ 的路穿过 $e$. 于是，如果 $x$，$y$ 是另一条边 $e'$ 的端点，则得到包含 $e$ 和 $e'$ 的一个多边形. 下面对边的总数(或秩)进行归纳来证明这一断言.

边为 $e$ 的连杆图是一个不可分子图. 设 $H$ 为包含 $e$ 的最大不可分的真子图. 如果 $x$ 和 $y$ 都在 $H$ 中，由归纳假设我们已完成证明. 否则，$G$ 是 $H$ 以及连结 $H$ 的顶点 $a$ 和 $b$ 的路图的并，假定 $x$ 和 $y$ 中至少有一个是 $P$ 的内部的顶点. 如果 $x$ 和 $y$ 都是 $P$ 的顶点，在 $H$ 中穿过 $e$ 的从 $a$ 到 $b$ 的路与 $P$ 的片段一起提供了所需的路. 最后，假设 $x$ 在 $P$ 的内部且 $y\in V(H)$. 比如说 $y\neq a$. 则在 $H$ 中从 $y$ 到 $a$ 穿过 $e$ 的一条路与 $P$ 的从 $x$ 到 $a$ 的片段合在一起提供了所需的路. 453

■

**推论** *一个不可分图 $G$(不是连杆图)的任意两个顶点包含在 $G$ 的某个多边形中.*

**证明** 对每个顶点选择一条边，如果这些边是不同的，应用定理 32.2. 如果这些边是相同的，只要这个图在其他地方有第二条边，就有一个多边形包含这条边. ■

这个推论实际上等价于定理 32.2. 因为在给定的边的中间插入新的顶点，然后对新的顶点应用推论就能导出定理.

这个推论是如下 H. Whitney(1932)的定理在 $k=2$ 时的特殊情形.

**定理 32.3** *一个至少有 $k+1$ 个顶点的图 $G$ 是 $k$-顶点连通的，当且仅当对 $G$ 的任意两个不同的顶点 $x$ 和 $y$，存在 $k$ 条内部不相交的路连结 $x$ 和 $y$，即除这些路的端点 $x$ 和 $y$ 之间，它们不共有其他顶点.*

这是下面的门格(Menger)定理的一个直接结论. 我们给出后者对有向图的表述. 如通常那样，当把每个无向边用一对有向边代替时，一个无向图可以视为一个有向图，一对有向边的每一条边指向一个方向.

下面对整数流应用定理 7.2，这需要如下的观察. (这几乎等同于问题 7B.)

**问题 32B** 设 $f$ 是有向图 $D$(容量没有要求)的一个从 $s$ 到 $t$ 的非负流.

(i)证明：如果 $f$ 有正强度，则存在从 $s$ 到 $t$ 的一条有向路，对它的所有边 $e$，$f(e)>0$.

(ii)得出结论：如果 $f$ 是整数且有强度 $k$，则在 $D$ 中存在 $k$ 条从 $s$ 到 $t$ 的有向路 $p_1$，$p_2$，…，$p_k$，使得对所有的边 $e\in E(D)$，穿过 $e$ 的路 $p_i$ 的数目 $\leqslant f(e)$.

**问题 32C** 在一个有向图 $D$ 中，设 $s$ 和 $t$ 是不同的顶点. 证明：从 $s$ 到 $t$ 的边不交的有向路的最大数目等于一个集合 $E$ 中的边的最小数目，$E$ 中边的删除使在那个方向上 $s$ 和 $t$ 不连通，即使得从 $s$ 到 $t$ 的每一条有向路至少包含 $E$ 的一条边.

454

在一个有向图 $D$ 中，设 $s$，$t$ 是两个不同的顶点. 一个 $(s, t)$-分离集是子集 $S\subseteq V(D)\setminus\{s, t\}$，使得从 $s$ 到 $t$ 的任意一条有向路至少包含 $S$ 的一个顶点.

**定理 32.4**（门格定理） *在一个有向图 $D$ 中，设 $s$，$t$ 是两个不同的顶点，并且假设没有边从 $s$ 指向 $t$. 如果没有规模小于 $k$ 的 $(s, t)$-分离集，则在 $D$ 中存在 $k$ 条从 $s$ 到 $t$ 的内部不交的有向路.*

**证明** 我们构造一个运输网络 $N$，它的顶点是 $s$，$t$，以及关于 $D$ 中除 $s$，$t$ 之外的每个点 $x$ 的一对新顶点 $x_1$，$x_2$. 对从 $s$ 指向 $D$ 的一个顶点 $x$ 的每条边，有 $N$ 的一条边，它从 $s$ 指向 $x_1$，且有无限容量（或任意的整数容量 $\geqslant k$）. 对从 $D$ 的一个顶点 $x$ 指向 $t$ 的每条边，有 $N$ 的一条边，它从 $x_2$ 指向 $t$ 且有无限容量. 对 $D$ 的从 $x$ 指向 $y$ 的每一条边 $e$，这里 $x$，$y$ 是 $D$ 中除 $s$，$t$ 之外的顶点，有一条从 $x_2$ 指向 $y_1$ 的有无限容量的一条边. 最后，对 $D$ 中除 $s$，$t$ 之外的每个顶点 $x$，有从 $x_1$ 指向 $x_2$ 的容量为 1 的一条边.

注意，由上面的构造方法，$N$ 中从 $s$ 到 $t$ 的一条有向路一定有形如

$$s, a_1, a_2, b_1, b_2, \cdots, z_1, z_2, t$$

的顶点项，这里 $s$，$a$，$b$，…，$z$，$t$ 是 $D$ 中从 $s$ 到 $t$ 的一条有向路的顶点项.

假设在 $N$ 中有从 $s$ 到 $t$ 的强度为 $k$ 的一个整数流 $f$. $f$ 的值可能仅仅为 0 和 1，因为 $N$ 的每一条边，或者进入顶点 $x_1$，对于这个顶点仅有的出边有容量 1；离开顶点 $x_2$，对 $x_2$ 仅有的入边有容量 1，或者是容量为 1 的边 $x_1\to x_2$. 由问题 32B，在 $N$ 中存在从 $s$ 到 $t$ 的 $k$ 条有向路的一个集合，这些路通过任意的边 $e$ 至多一次. 这些路是边不交的，因此是内部不相交的，因为共有两个顶点 $x_1$ 和 $x_2$ 的两条有向路一定共有一条边 $x_1\to x_2$. 于是，在 $D$ 中对应的 $k$ 条路是内部不相交的.

455

为保证这样的流 $f$ 存在，我们考虑 $N$ 中隔开 $s$ 和 $t$ 的一个割 $(S, T)$，为引出矛盾，假设这个割的容量 $<k$. $N$ 中容量可能小于 $k$ 的边仅仅是那些对 $x\in V(D)$，从 $x_1$ 指向 $x_2$ 的边. 如果设 $V$ 是 $D$ 的顶点 $x$ 的一个集合，它使得 $x_1\in S$ 且 $x_2\in T$，那么这个割的容量是 $|V|$. 在 $N$ 中从 $s$ 到 $t$ 的每一条有向路一定通过这些边 $x_1\to x_2$ 中的一条. 等价地，$D$ 中的每一条有向路一定通过 $V$ 的一个顶点 $x$，于是 $V$ 是一个 $(s, t)$-分离集. 如果定理的假设成立，我们就得到一个矛盾. ■

* * *

在 $\mathbb{R}^n$ 中，一个凸多胞形（也称凸多面体）$P$ 是有限个点的凸包，即

$$P=\{\lambda_1\boldsymbol{x}_1+\cdots+\lambda_k\boldsymbol{x}_k : \lambda_i\geqslant 0, \lambda_1+\cdots+\lambda_k=1\}.$$

一个凸多胞形的维数是它的仿射生成的维数.

$P$ 的支撑超平面是超平面

$$H = \{\boldsymbol{x} : \ell(\boldsymbol{x}) = c\}$$

(这里 $\ell$ 是一个非零的线性泛函$\mathbb{R}^n \to \mathbb{R}$，且 $c$ 是一个标量)，$H \cap P \neq \varnothing$，但使得 $P$ 完全位于 $H$ 的闭半空间之中，比如说

$$P \subseteq \{\boldsymbol{x} : \ell(\boldsymbol{x}) \geqslant c\}.$$

$P$ 的面是 $P$ 的支撑超平面与 $P$ 的交(尽管经常把空集作为一个面)．$P$ 的顶点是 0 维的面，$P$ 的边是 1 维的面．多胞形 $P$ 的图 $G$(也称为 $P$ 的 1-骨架)是 $V(G)$和 $E(G)$分别等于 $P$ 的顶点和边，关联性由包含确定．

面 $F$ 自身是一个凸多胞形；事实上，它是 $P$ 的顶点的凸包，这些顶点被它包含(参见 Grünbaum，1967)．$F$ 的图是 $P$ 的图的一个子图．

456

下面的结果属于 M. Balinski(1961)．对它的证明，我们需要以下来自线性规划理论的事实；参见 Grünbaum(1967)．如果 $s$ 是$\mathbb{R}^m$中的多胞形 $P$ 的一个顶点，$\ell$ 是一个线性泛函，或者对所有的 $x \in P$ 有 $\ell(s) \geqslant \ell(x)$，或者存在与 $s$ 相邻的 $P$ 的一个顶点 $t$ 使得 $\ell(t) > \ell(s)$．

**定理 32.5** $n$ 维凸多胞形的图 $G$ 是 $n$-连通的．

**证明** 我们对 $n$ 用归纳法．一个 0 维多胞形由单独一个点构成．1 维多胞形由两个顶点和连结它们的一条边组成．

设 $x_1$，$x_2$，$\cdots x_{n-1}$，$a$，$b$ 是图 $G$ 的不同顶点，$G$ 是维数为 $n$ 的一个凸多胞形 $P$ 的图．可以假设 $P \subseteq \mathbb{R}^n$．我们想在 $G$ 中找出从 $a$ 到 $b$ 但避开顶点 $x_1$，$\cdots$，$x_{n-1}$的一条路径．选择包含 $x_1$，$\cdots$，$x_{n-1}$的一个$(n-2)$维的仿射空间 $S$．有一个超平面 $H$，即一个$(n-1)$维的仿射子空间，它在 $S$ 上使得 $a$ 和 $b$ 都在 $H$ 的同一侧，即对某个$\mathbb{R}^n$上的线性泛函 $\ell$ 和某个标量 $\alpha$，$H = \{z : \ell(z) = \alpha\}$ 且 $\ell(a) \geqslant \alpha$，$\ell(b) \geqslant \alpha$．($a$，$b$ 中的一个或两者都在 $H$ 中是允许的．)

因为 $P \not\subseteq H$，所以可以假设 $P$ 包含使 $\ell(z) > \alpha$ 的点 $z$(否则 $a$ 和 $b$ 在 $H$ 中，并且可以由 $\ell$ 和 $\alpha$ 的相反数代替它们——即考虑 $H$ 的另一侧)．

由上面来自线性规划理论的事实，在 $G$ 中存在分别从 $a$ 和 $b$ 到顶点 $a'$和 $b'$的路 $p$ 和 $q$，$\ell$ 在路上的点取得最大值 $\alpha'$，并且使得 $p$ 和 $q$ 除了它们的起始顶点之外都不在 $H$ 中．交 $P \cap H'$(这里 $H' := \{z : \ell(z) = \alpha'\}$)是 $P$ 的一个面，维数至多为 $n-1$，而且特别地包含一个连通图，所以在 $G$ 中存在从 $a'$到 $b'$且顶点在 $H'$中的一条路 $r$．我们连接 $p$，$r$，以及 $q$ 的反转，就得到了从 $a$ 到 $b$ 的一条路径． ■

**问题 32D** 说一个图 $G$ 是 $k$-塔特-连通的，若对每个 $\ell < k$，不可能找到 $G$ 的一对非空的边不交的子图$(H, K)$，每一个至少包含 $\ell$ 条边，使得 $H \cup K = G$ 且 $|V(H) \cap V(K)| = \ell$．这样的一对子图可以称为 $G$ 的 $\ell$-分离．顶点-连通性和塔特-连通性的概念是不同的．但容易看出，对于一个非空的图，1-塔特-连通性与通常的连通性是相同的，而且 2-塔特-连通性与不可分性是相同的．一个至少有两条边的 2-塔特-连通图不能有环，否则我们有两个边不交的子图(一个是环图，另一个是包含所有其他边的图)，每一个至少有一条边，但只有一个公共的顶点．证明对 $|V(G)| \geqslant k+1$ 的一个图 $G$，$G$ 是 $k$-塔特-连通的，当且仅当 $G$ 是 $k$-顶点连通的且没有边数少于 $k$ 的多边形．

457

## 评注

参见第 34 章的评注中对惠特尼(H. Whitney)的一些评论.

门格(Karl Menger, 1902—1985)是奥地利数学家，1937 年他离开奥地利赴美，在美国度过了他的余生. 他致身于逻辑学、教学法和经济学等诸多领域，但是最著名的是关于维数论和曲线论的工作. 获得哲学博士学位后，他在阿姆斯特丹与布劳威尔(L. E. J. Brouwer)一起工作，1927 年他作为一名教授返回维也纳. 在维也纳，他创立了包括 K. Gödel 和 A. Wald 在内的著名成员以及大量访问者的维也纳数学论坛(the Vienna Mathematical Colloquium). 在该论坛由于许多投稿者是犹太人而被迫停止之前，他们的成果出版了八卷.

## 参考文献

M. Balinski (1961), On the graph structure of convex polyhedra in $n$-space, *Pacific J. Math.* **11**, 431–434.

L. R. Ford, Jr. and D. R. Fulkerson (1962), *Flows in Networks*, Princeton University Press.

B. Grünbaum (1967), *Convex Polytopes*, J. Wiley (Interscience).

H. Whitney (1932), Nonseparable and planar graphs, *Trans. Amer. Math. Soc.* **34**, 339–362.

458

# 第33章　平面性和染色

我们以关于删除和收缩的材料开始．在下一章中将会讨论一些"对偶"概念；参见问题 34C.

设 $G$ 为一个图且 $e \in E(G)$．我们以相同的边集 $E(G) \setminus \{e\}$ 定义两个图 $G'_e$ 和 $G''_e$．第一个图 $G'_e$ 由 $G$ 删除边 $e$ 得到．（此后移去可能出现的孤立顶点有时是方便的，但我们允许保留孤立顶点.）第二个图 $G''_e$ 由等同 $e$ 的端点并移去 $e$ 自身得到．在一个图的图示中，我们可以想象一条边"绕在一起"或"收缩"，如图 33.1 所示．

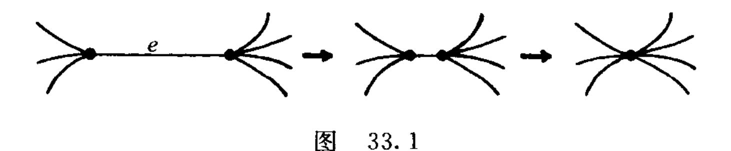



图　33.1

一个有限图 $G$ 的色多项式 $\chi_G$ 已在第 25 章中引入：$\chi_G(\lambda)$是用 $\lambda$ 种颜色对 $G$ 正常染色的数目．例如，注意到

$$\chi_{K_n}(\lambda) = \lambda(\lambda-1)(\lambda-2)\cdots(\lambda-n+1).$$

$\chi_G$ 是 $\lambda$ 的多项式已在第 25 章加以证明——也见(33.1)后的注释.

**例 33.1**　我们断言对 $n$ 个顶点的一棵树 $T$，

$$\chi_T(\lambda) = \lambda(\lambda-1)^{n-1}.$$



为了明白这一点，观察到如果 $x$ 是 $T$ 的一个一价顶点，在移去 $x$ 的 $n-1$ 个顶点的树有一个正常染色之后，有 $\lambda-1$ 种颜色可供 $x$ 使用．断言由对顶点的数目进行归纳得到.

如果 $e$ 是 $G$ 的一条边，它不是环，可以把 $G'_e$ 的正常染色分成两类：$e$ 的端点着不同的色(这些是 $G$ 的正常染色)和 $e$ 的端点着相同的色(这些与 $G''_e$ 的正常染色一一对应)．由此建立

$$\chi_G(\lambda) = \chi_{G'_e}(\lambda) - \chi_{G''_e}(\lambda). \tag{33.1}$$

等式(33.1)提供了理解 $\chi_G(\lambda)$是 $\lambda$ 的一个多项式的另一条途径．有环的图 $H$ 没有正常染色，即 $\chi_H(\lambda)=0$．对 $n$ 个顶点的无边图 $H$，$\chi_H(\lambda)=\lambda^n$．两者都是多项式．现在对图的边数使用(33.1)和归纳法.

一棵树 $T$ 的色多项式也可由归纳法和(33.1)得到：$T''_e$ 是一棵树且 $T'_e$ 有两个部分是树.

**问题 33A**　设 $\tau(G)$表示一个图 $G$ 的生成树的数目(有时这被称作 $G$ 的*复杂度*)．证明对任意的非环边 $e \in E(G)$，$\tau(G)=\tau(G'_e)+\tau(G''_e)$.

**问题 33B**　求 $n$-边形 $C_n$ 的色多项式．求 $n$-轮 $W_n$(即由 $C_n$ 添加一个新的顶点并把它与 $C_n$ 的所有顶点连结得到的图)的色多项式.

对一个图，求图用 $-1$ 种颜色的正常染色的数目是没有意义的，但是，因为 $\chi_G(\lambda)$是一个多项式，我们可以计算 $\chi_G(-1)$．R. P. Stanley(1973)发现 $|\chi_G(-1)|$ 的一个组合解释如下．一个图的*定向*是这样一个有向图，即对图中每条边选择一个端点为头，另一个端点为尾产生的有

向图.（于是有 $m$ 条边的无环图的定向数是 $2^m$——尽管为了拓扑学的目的，应允许环有两个方向.）

460

**定理 33.1** 一个图 $G$ 的无圈定向(即在定向中没有有向的回路)数是$(-1)^{|V(G)|}\chi_G(-1)$.

**证明** 如果 $G$ 有环，则 $\chi_G(\lambda)=0$ 且 $G$ 没有无圈的定向，于是在这种情形定理成立.

考虑 $G'_e$ 的一个无圈定向，这里 $e$ 不是一个环. 为得到 $G$ 的一个定向，有两种方法给 $e$ 定向. 我们断言它们中的一个或者两者是无圈的，且在两者都是无圈的情形与 $G''_e$ 的无圈定向一一对应. 这是因为从一个端点 $x$ 到另一个端点 $y$ 的 $e$ 的定向产生一个非无圈定向，当且仅当在 $G'_e$ 中从 $y$ 到 $x$ 有一条有向路；在 $G'_e$ 中，从 $x$ 到 $y$ 且从 $y$ 到 $x$ 没有有向路，因为我们假定了一个无圈定向；再者，在 $G'_e$ 中从 $y$ 到 $x$ 没有有向路，当且仅当等同 $x$ 和 $y$ 产生 $G''_e$ 的一个无圈定向.

于是

$$\omega(G) = \omega(G'_e) + \omega(G''_e),$$

这里 $\omega(H)$取作一个图 $H$ 的无圈定向数. 但由(33.1)，当 $\omega(H)$被取作$(-1)^{|V(H)|}\chi_H(-1)$时，这个相同的递归式也都满足. 在对无边图检验定理成立之后，由对边数的归纳法得到这个定理. ■

一个图 $G$ 在曲面 $S$ 上的嵌入或适当的画法，是指边不交叉且只在顶点相遇的一种画法. 更精确地，是指图的一个表示，其中顶点对应于 $S$ 中的点，边对应于连结 $S$ 上的点的若尔当弧(单位区间的连续的一一对应)，被连结的 $S$ 上的点与 $G$ 中边的端点对应，而且任何一条若尔当弧的中间的点不是另一条若尔当弧的顶点或者对应于 $G$ 中顶点的点. 我们只考虑有限图的嵌入. 由于平面不是紧致的，它能自然地嵌入在球中(它的一个点紧致化)，而且一个图是平面的，当且仅当它能嵌入在球上.

461

不是平面图的例子包括 $K_{3,3}$和 $K_5$；后面我们将提到认识这一点的几种途径. 这些图的细化，而且包含这些细化中任一个的图，也不是平面的. 一个重要的但我们不给出证明的定理如下. 证明可在 Chartrand and Lesniak(1986)、Tutte(1984)以及 Diestel(1997)中找到.

**定理 33.2**(Kuratowski) 一个图 $G$ 是平面的，当且仅当它没有同构于 $K_5$ 或 $K_{3,3}$的细化的子图.

**问题 33C** 找出作为彼得森图的子图的 $K_{3,3}$的一个细化.

图 $G$ 的一个缩减图(或子式)是图 $H$，它由 $G$ 通过删除和收缩边，以及此后可能删除某个或所有孤立的顶点而得到.

可以看出，边的删除或收缩顺序是不重要的. 例如，如果边的子集 $S\subseteq E(G)$以任意顺序收缩，得到一个同构于图 $G''_S$ 的图，$G''_S$ 称为 $G$ 的收缩，定义如下. 正式地，$G''_S$ 的顶点是由边集 $S$ 生成的 $G$ 的支撑子图的分支，记为 $G:S$. $G''_S$ 的边集是 $E(G)\setminus S$. 在 $G''_S$ 中，边 $e\in E(G)\setminus S$ 的端点是 $e$ 作为 $G$ 的边包含 $e$ 的端点的 $G:S$ 的分支. 非正式地，$G:S$ 的分支被缩为单独的点.

我们用记号 $G'_S$ 表示删去 $S$ 中的边得到的图，即 $G:(E(G)\setminus S)$，当应用这个记号时删去孤立的顶点是方便的.

**例 33.2** 设 $A$ 是图 1.4 的左侧通常画彼得森图 $P$ 时的五个“轮辐”. 子图 $P:A$ 有五个分

支，因此 $P''_A$ 有五个顶点. 在这种情况下，图的收缩 $G''_S$ 是 $K_5$. 如果 $B$ 是内部的五角星形的五条边的集合，则 $P:B$ 有六个分支且 $P''_B$ 是轮 $W_5$. 如果 $C$ 是 $P$ 的支撑树的边集，则 $P''_C$ 由一个单独的顶点和六个环构成.（有一个顶点的图可以称之为余树.）

注意，$G''_S$常有环和/或平行边，即使 $G$ 是简单图.（一个简单图 $G$ 的收缩没有环，该收缩与格 $\Pi(G)$的元素一一对应，这个格是在例 23.6 中引入的划分格的子格.） 462

图 $G$ 是其任意一个细分 $H$ 的收缩，因为有 $k$ 条边的路图的任意 $k-1$ 条边的收缩产生一个连杆图.

如果在曲面$\mathcal{S}$上有图 $G$ 的一个图示且 $e\in E(G)$，显然在$\mathcal{S}$上有 $G'_e$ 的一个自然的图示. 如果 $e$ 不是一个环，在$\mathcal{S}$上也有 $G''_e$ 的一个自然导出的图示：在曲面$\mathcal{S}$上该边的端点可以不断靠近（见图 33.1）.（按照我们的组合定义，一个环的收缩与删去它是一样的.）特别地，如果允许 $G$ 嵌入到曲面$\mathcal{S}$上，则 $G$ 的每个缩减图也能嵌入到$\mathcal{S}$上.

**问题 33D** 证明有一个缩减图同构于 $K_5$ 或 $K_{3,3}$的图 $G$ 也包含 $K_5$ 或 $K_{3,3}$的一个细化. 更一般些，证明：

(i)如果一个三值图 $H$ 作为图$G$ 的一个缩减图出现，则 $G$ 包含(作为一个子图)$H$ 的一个细化. 于是，如果 $K_{3,3}$是一个缩减图，则 $K_{3,3}$的细化是一个子图.

(ii)如果 $K_5$ 是 $G$ 的一个缩减图，则 $G$ 包含 $K_5$ 或 $K_{3,3}$的一个细化.

属于 N. Robertson 和 P. Seymour 的一个深刻且极为重要的定理说，在图的每个无穷集合中，存在两个图使得一个是另一个的缩减图. 对这项工作的部分讨论，见 Diestel(1997)的第12 章. 由此得出：在一个给定的曲面上不能嵌入的且相对于这个性质是最小的图(每个正常或真的缩减图是可嵌入的)的集合是有限集. 对于平面，有两个.

在曲面$\mathcal{S}$上给定图 $G$ 的一个嵌入，相对于这个嵌入我们定义表面或区域是从$\mathcal{S}$移去顶点和边(更精确一些，对应于顶点的点和对应于边的若尔当孤上的点集)产生的在拓扑上连通的分支. 面的集合由 $F(G)$表示. 我们认识到这是一个可怕的记号，因为面依赖于嵌入(特别地，嵌入的曲面)且一般地不能由 $G$ 确定. 但我们还是使用这个记号. 463

一般来说，这些面可能是也可能不是 2-胞腔.（与“没有洞”的开单位圆盘同胚）. 但对球上的一个连通图的嵌入，区域将是 2-胞腔. 这个事实与若尔当曲线定理有关，它断言如果球上单位圆的一个一一对应的连续映象的点被移去，得到的拓扑空间恰有两个简单的连通分支，它们是 2-胞腔.

**定理 33.3**(欧拉公式) *对球或平面上画出的连通平面图 $G$，则*

$$f-e+v=2,$$

*这里 $f$，$e$ 和 $v$ 分别是面、边和顶点的数目. 更一般地，对嵌入到球上的任意图 $G$，*

$$1-|F(G)|+|E(G)|-|V(G)|+|C(G)|=0, \tag{33.2}$$

*这里 $C(G)$表示 $G$ 的分支的集合.*

**证明** 我们对 $G$ 的边数用归纳法证明后一个断言. 对无边图 $G$，$|C(G)|=|V(G)|$ 且 $|F(G)|=1$，于是(33.2)成立.

假设 $G$ 有一个非环的边 $a$. 考虑 $G$ 的一个嵌入并注意到收缩一条边不影响面的数目. 应用

归纳假设于 $G''_a$ 以得到

$$1-|F(G''_a)|+|E(G''_a)|-|V(G''_a)|+|C(G''_a)|=0.$$

我们有 $|E(G)|=|E(G''_a)|+1$，$|V(G)|=|V(G''_a)|+1$，$|C(G)|=|C(G''_a)|$，而且 $|F(G)|=|F(G''_a)|$. 因此对 $G$，(33.2)成立.

假设 $G$ 有环，设 $a$ 为环中的一个，应用归纳假设于 $G'_a$ 以得到

$$1-|F(G'_a)|+|E(G'_a)|-|V(G'_a)|+|C(G'_a)|=0.$$

当然 $|E(G)|=|E(G'_a)|+1$，$|V(G)|=|V(G'_a)|$，且 $|C(G)|=|C(G'_a)|$. 在球上，若尔当曲线定理蕴涵与 $e$ 关联的两个面是不同的，于是 $|F(G)|=|F(G'_a)|+1$，对 $G$ 我们得到(33.2). ■

464

**例 33.3** 我们证明 $K_5$ 和 $K_{3,3}$不是平面的，在一个不可分的平面图(连杆图除外)的平面嵌入中，与一个面关联的边的集合包含一个多边形子图，见第 34 章. 一个面的度是与它关联的边的数目(即第 34 章的对偶图的顶点的度数). 因为每条边与两个面关联，面的度数的和是边的数目的两倍.

考虑 $K_5$ 在平面上的一个假设的嵌入. 由欧拉公式，它有七个面. 但每个面的度至少为 3，于是面的度之和至少为 21，这当然与 $|E(K_5)|=10$ 矛盾.

类似地，$K_{3,3}$在平面上的一个假设的嵌入有五个面，因为 $K_{3,3}$的围长为 4. 每个面的度至少为 4. 那么面的度之和至少为 20，与 $|E(K_{3,3})|=9$ 矛盾.

(一个类似的论证证明彼得森图不是平面的. 但我们已经知道这一点，因为作为彼得森图的缩减图出现的 $K_5$ 和 $K_{3,3}$都不是平面图.)

**问题 33E** 确定整数的所用对$(d_1, d_2)$，这里 $d_i\geqslant 2$，$i=1, 2$，使得存在一个平面图(不一定是简单的)，它是 $d_1$ 度正则的且所有面的度为 $d_2$. (这将包括五个柏拉图(Platon)立体的顶点和面的度.)

E. Steinitz(1922)刻画了 3-维凸多面体的图.

**定理 33.4** *图 $G$ 是一个 3-维凸多面体的图，当且仅当 $G$ 是简单的、平面的和 3-连通的.*

一个 3-维多面体是 3-连通的是定理 32.5 的一个特殊情形. 我们不证明该定理的其余部分.

问题“能用四种或更少的颜色给画在球面上的地图中的国家染色，使得相邻的国家染的颜色不同吗?”出现在德摩根(Augustus de Morgan)致哈密顿(William Rowan Hamilton)爵士的一封信中，日期为 1852 年 10 月 23 日. 问题的提出者似乎是德摩根的学生 Frederick Guthrie 的兄弟 Francis Guthrie.

465

一个平面地图的国家(区域)的染色等价于该图的对偶图的顶点的染色，对偶图将在下一章介绍. 因此，“四色问题”是每个平面图是否四色可染的问题.

显然四种颜色是必要的，因为 $K_4$ 是平面图，而且容易发现许多其他的平面图 $G$ 不是 3-可染色的. 这个问题激发了图论中的许多研究. 关于四色问题历史的更多内容可在 Biggs, Lloyd, and Wilson(1976)中找到.

1890 年，P. J. Heawood 证明了五色定理(即定理 33.6)：一个无环的平面图 $G$ 的色数 $\chi(G)\leqslant 5$. Heawood 利用了 A. B. Kempe 的想法(特别是下面评论的重新染色的想法). 1976 年，K. Appel 和 W. Haken 发布了四色定理 $\chi(G)\leqslant 4$ 的证明，从而最终解决了四色问题. 令人吃惊的也许是，他们的工作没有大量地利用在 20 世纪发展的许多工作和理论，而是回到 Kempe 和 Heawood 的想法. 另一个惊人的地方是，他们的工作需要超过 1000 小时的计算机时间. 当他们开始时并不清楚计算会最终停止. 作为一个过度的简化，有许多情形需要考虑，但并不确定它们的数目是有限的；计算机依照程序产生情形自身，而且令人信服地不断将情形分为子情形. 见 Appel，Haken，and Koch(1977)，以及 Appel and Haken(1977). 限于篇幅，这里不详细讨论这一工作，但证明五色定理如下.

**命题 33.5** 每个非空的简单平面图 $G$ 有一个顶点的度至多为 5.

**证明** 这可以从欧拉公式很快得出. 证明一个分支有这样一个顶点就够了，因此假设 $G$ 是连通的. 假设 $G$ 的图示有 $f$ 个区域、$e$ 条边和 $v$ 个顶点. 如果没有度小于 6 的顶点存在，则 $v$ 个顶点的度之和至少为 $6v$，这个和等于 $2e$；这就是

$$v\leqslant \frac{e}{3}.$$

因为 $G$ 是简单图(且可以假设它不是两个顶点由单独一条边连结的连杆图)，每个区域至少与三条边关联，所以 $G^*$ 的 $f$ 个顶点的度之和至少为 $3v$，这个和等于 $2e$；这就是 [466]

$$f\leqslant \frac{2e}{3}.$$

但是，出现矛盾

$$2=f-e+v\leqslant \frac{e}{3}-e+\frac{2e}{3}=0. \qquad \blacksquare$$

当然，无环图的染色等价于简单图的染色(不过取消多重边). 上面结果的一个直接结论是六色定理：一个无环的平面图 $G$ 有 $\chi(G)\leqslant 6$. 当度至多为 5 的一个顶点 $x$ 被从一个简单平面图中删去，用 6 种颜色归纳地给得到的图染色时，总有一种颜色可供给 $x$.

回忆第 3 章介绍的重新染色的思想. 假定 $G$ 被正常地染色，设 $\alpha$ 和 $\beta$ 是两种颜色. 在由染 $\alpha$ 和 $\beta$ 的顶点导出的子图的任意分支中，交换颜色 $\alpha$ 和 $\beta$ 能得到另一个正常的染色. 因此，给定颜色分别为 $\alpha$ 和 $\beta$ 的顶点 $x$ 和 $y$，或者有顶点为 $a_0=x$，$a_1$，…，$a_n=y$ 的交错染颜色 $\alpha$ 和 $\beta$ 的一条(奇长度的)路(所谓的 Kempe 链)，或者有一个正常的染色，其中 $x$ 和 $y$ 的颜色都是 $\alpha$，即是说，染 $\alpha$ 和 $\beta$ 之外的其他顶点保持原来的颜色.

**定理 33.6** 如果 $G$ 是一个无环的平面图，则 $\chi(G)\leqslant 5$.

**证明** 我们对顶点的数目用归纳法. 该断言对至多有 5 个顶点的图无疑是正确的. 考虑一个无环平面图 $G$ 的平面图示，假设定理对少一个顶点的所有图成立. 假设 $G$ 是简单的.

由命题 33.5，存在一个度 $\leqslant 5$ 的顶点 $x\in V(G)$. 设 $G_x$ 是从 $G$ 删去 $x$ 及 $x$ 关联的边得到的图. 从 $G$ 的图示可以得到 $G_x$ 的自然的平面图示. 由归纳假设，$G_x$ 有用 5 种颜色的一个正常染色. 对 $x$ 有一个可用的颜色，我们就完成了染色，除非 $x$ 的度恰为 5 且在 $G$ 中与 $x$ 相邻的 5 个点 $y_1$，$y_2$，…，$y_5$(按图示给定的循环顺序写出)在 $G_x$ 的染色中得到 5 种不同的颜色. 于是 [467]

假设 $y_i$ 得到颜色 $i$，$i=1, 2, 3, 4, 5$. 见图 33.2.

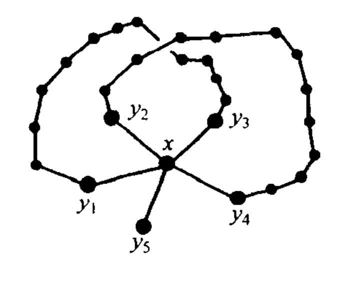


图 33.2

考虑颜色 1 和 3. 或者存在 $G_x$ 的一个正常染色，其中 $y_1$ 和 $y_3$ 都有颜色 1(同时 $y_2$，$y_4$ 和 $y_5$ 保持它们原来的颜色)，或者在 $G_x$ 中存在一条顶点交错染颜色 1 和 3 的简单路，比如说

$$y_1, a_1, b_1, a_2, b_2, \cdots, a_s, b_s, y_3. \tag{33.3}$$

在第一种情形，赋予 $x$ 颜色 3，我们完成染色. 类似地，或者存在 $G_x$ 的一个正常染色，其中 $y_2$ 和 $y_4$ 都有颜色 2(同时 $y_1$，$y_3$ 和 $y_5$ 保持它们原来的颜色)，或者在 $G_x$ 中存在一条顶点交错染颜色 2 和 4 的简单路，比如说

$$y_2, c_1, d_1, c_2, d_2, \cdots, c_t, d_t, y_4. \tag{33.4}$$

在第一种情形，赋予 $x$ 颜色 4，我们完成染色.

为了完成证明，注意上面的两条路不能同时存在. 如果(33.3)中的路存在，则

$$x, y_1, a_1, b_1, a_2, b_2, \cdots, a_s, b_s, y_3, x \tag{33.5}$$

是一条简单闭路的顶点序列，它们把平面分为两个区域. 顶点 $y_2$ 在一个区域同时 $y_4$ 在另一个区域. 在 $G_x$ 中从 $y_2$ 到 $y_4$ 的任意一条路必定与(33.4)的路有一个公共的顶点，且特别地一定有颜色为 1 或 3 的一个顶点；因此如(33.5)中的序列不存在. ■ 468

在第 17 章，处理了图的目录染色，目的是解释 Dinitz 猜想的 Galvin 证明. 下面讨论 C. Thomassen(1994)的一个结果，它通过首先给图的每个顶点一个 5 种不同颜色的目录，每个顶点的目录不必是相同的，为五色定理提供了第二种证明. 应特别注意证明中的一个思路，它常用来使证明变得容易. 这个思路涉及作出更严格的归纳假设，从而使归纳步骤更为容易.

**定理 33.7** *设 $G$ 是有 $N$ 个顶点 $v_1$，$v_2$，…，$v_N$ 的一个平面图. 对 $i=1$，…，$N$，设 $S_i$ 为 5 个元素(可称之为颜色)的一个集合. 存在顶点上的一个映射 $f$，$f(v_i)\in S_i$，使得对所有相邻的点对 $v_i$，$v_j$ 有 $f(v_i)\neq f(v_j)$($G$ 的一个五目录染色).*

**证明** 首先通过增加额外的边使问题更难，增加的边使 $G$ 变成三角剖分多边形. 设标号使得 $v_1$，$v_2$，…，$v_k$ 是该多边形相继的顶点(见图 33.3). 对这些顶点中的每一个，从其目录中移去两种颜色，以便多边形周界上的顶点仅有三种可用颜色的目录. 问题再次变得更为困难. 最后，在多边形的周界上选相邻两个点并从它们的目录中赋予每个点一种颜色，这是进一步的限制. 我们断言，由这些初始条件可完成染色. 证明是对顶点的数目用归纳法(数目少的情形是平凡的). 469

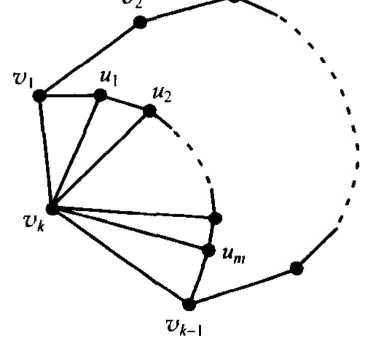


图 33.3

对归纳，区分两种情形. 在第一种情形，假设多边形有一条边连结周界上不相邻的两个顶点，即一条弦. 这条弦把多边形分为两部分，其中的一部分包含两个预先染色的顶点(一个染色的顶点可能作为弦的一个端点). 这一部分的染色由归纳假设可以完成. 从这一部分的染色，另一部分继承了周界上相邻两个点的染色，因此又由归纳完成该部分的染色.

现在假设不存在弦. 设 $v_1$ 和 $v_2$ 是周界上被预先染色的顶点，并设 $v_1$，$u_1$，$u_2$，…，$u_m$，

$v_{k-1}$为按顺序(顺时针，见图 33.3)邻接到 $v_k$ 的顶点，顶点 $u_i$ 为内部的顶点，又由于三角剖分，有边$(v_1, u_1)$，$(u_1, u_2)$，$\cdots(u_{m-1}, u_m)$，$(u_m, v_{k-1})$. $v_k$ 的目录至少有两种颜色不等于 $v_1$ 的颜色. 我们取这两种颜色并从 $u_1$ 到 $u_m$ 的目录中移去这两种颜色，如果必要，把这些目录缩短到规模为 3. 由归纳法，可以完成 $G\setminus\{v_k\}$的染色. 可能 $v_{k-1}$已得到了 $v_k$ 的目录中的两种颜色之一，但余下的一种用于完成 $G$ 的染色. ■

## 评注

1872 年，A. B. Kempe(1849—1922)以优异的数学成绩在剑桥大学三一学院获得学位，同时他也以出众的男高音赢得了音乐方面的声誉. 在不放弃数学研究的同时，他选择法律为职业. [470]

波兰数学家 Kazimierz (或 Casimir) Kuratowski(1896—1980)于 1966 年退休之前一直在华沙大学(几近 40 年)和 Lwow 工学院任教. 他的刻画平面图性质的定理是在 1930 年证明的.

Ernst Steinitz(1871—1928)是波兰布雷斯劳(今弗罗茨瓦夫)和德国基尔的教授. 他(与希尔伯特)对域论做出了重要贡献.

1993 年，M. Voigt 发现了有 238 个顶点的一个平面图不是四目录可染色的例子.

## 参考文献

K. Appel and W. Haken (1977), The solution of the four-color map problem, *Scientific American* **237**, 108–121.

K. Appel, W. Haken, and J. Koch (1977), Every planar map is four colorable, *Illinois J. Math.* **21**, 429–567.

N. L. Biggs, E. K. Lloyd, and R. J. Wilson (1976), *Graph Theory 1736–1936*, Oxford University Press.

G. Chartrand and L. Lesniak (1986), *Graphs and Digraphs*, 2nd edn., Wadsworth.

R. Diestel (1997), *Graph Theory*, Springer-Verlag Graduate Texts in Mathematics **173**.

R. P. Stanley (1973), *Acyclic orientations of graphs*, Discrete Math. **5**, 171–178.

E. Steinitz (1922), Polyeder und Raumeinteilungen, *Enzykl. Math. Wiss.* **3**, 1–139.

C. Thomassen (1994), Every planar graph is 5-choosable, *J. Combin. Theory Ser. B* **62**, 180–181.

W. T. Tutte (1984), *Graph Theory*, Encylopedia of Math. and its Appl. **21**, Addison-Wesley. Reissued by Cambridge University Press.

[471]

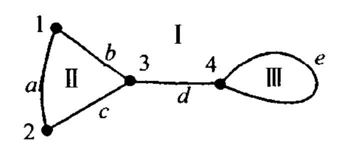
# 第34章　惠特尼对偶

一条若尔当弧把一个小邻域内的点分为两"半"．在一张地图中，一条边除了与两个顶点(它们可能重合)相关联外，还与两个区域(它们可能重合)相关联．见图 34.1.

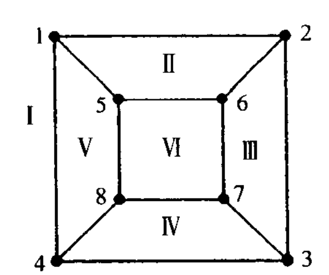
图 34.1

这允许我们相对于 $G$ 的一个 2-胞腔在曲面 $\mathcal{S}$ 上的嵌入定义图 $G$ 的对偶图 $G^*$．图 $G^*$ 的顶点 $V(G^*)$ 是相对于嵌入的区域；边 $E(G^*)$ 与 $G$ 的边相同；在 $G^*$ 中边 $e$ 的端点是与 $e$ 相关联的区域．图 34.2 中展示了两个例子.

我们已抽象地定义了 $G^*$，注意到允许 $G^*$ 嵌入在同一曲面 $\mathcal{S}$ 上是重要的：一个区域由它内部的一个点表示，两个共享一条边 $e$ 的区域的内部的点由只与 $G$ 中表示 $e$ 的若尔当弧相交的一条若尔当弧表示．图 34.2 中立方体的对偶的图示显示在图 34.3 中.




| $G$ 中的端点 | 边 | $G^*$ 中的端点 |
|---|---|---|
| 1，2 | $a$ | Ⅰ，Ⅱ |
| 1，3 | $b$ | Ⅰ，Ⅱ |
| 2，3 | $c$ | Ⅰ，Ⅱ |
| 3，4 | $d$ | Ⅰ，Ⅰ |
| 4，4 | $e$ | Ⅰ，Ⅲ |




| $G$ 中的端点 | 边 | $G^*$ 中的端点 |
|---|---|---|
| 1，2 | $a$ | Ⅰ，Ⅱ |
| 2，3 | $b$ | Ⅰ，Ⅲ |
| 3，4 | $c$ | Ⅰ，Ⅳ |
| 4，1 | $d$ | Ⅰ，Ⅴ |
| 5，6 | $e$ | Ⅱ，Ⅵ |
| 6，7 | $f$ | Ⅲ，Ⅵ |
| 7，8 | $g$ | Ⅳ，Ⅵ |
| 8，5 | $h$ | Ⅴ，Ⅵ |
| 1，5 | $i$ | Ⅱ，Ⅴ |
| 2，6 | $j$ | Ⅱ，Ⅲ |
| 3，7 | $k$ | Ⅲ，Ⅳ |
| 4，8 | $l$ | Ⅳ，Ⅴ |

图　34.2

例子将使读者相信 $(G^*)^*$ 同构于 G．我们请读者思考但不要求读者正式证明的两个事实是：一个不连通的图没有 2-胞腔嵌入；相对于一个 2-胞腔嵌入的对偶图总是连通的.

472～473

多边形系列的平面对偶是键图，即有两个顶点和任意正数条边连结它们的图．特别地，环图和连杆图是对偶的．树的平面对偶是余树，余树的平面对偶是树.

一般地，一个图可能有几个平面对偶图. 图 34.4 显示了两个同构的余树，以及相对于两个嵌入，它们的不同构的平面对偶. 图 34.5 显示了一个不可分图 $G$ 的嵌入和相对于每个嵌入的对偶图，它们不同构.

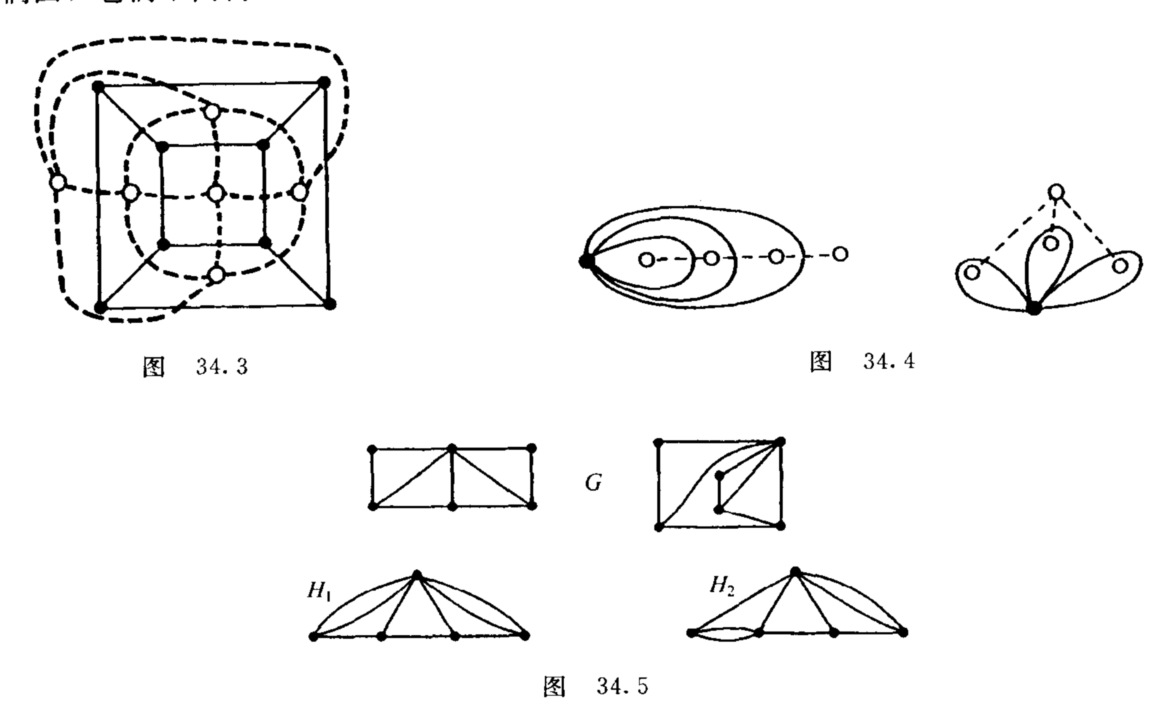



图 34.3

图 34.4

图 34.5

本章的目的是“组合地”理解一个平面图和它的对偶图之间的关系. 我们将利用这一理解(惠特尼对偶)证明关于平面图和它们的对偶的几个定理(不涉及平面图示或拓扑). 474

回忆图 $G$ 的关联矩阵 $N=N(G)$ 是其行由 $V(G)$ 指示、其列由 $E(G)$ 指示的矩阵，这里

$$N(x,e)=\begin{cases}1 & \text{如果 } x \text{ 与一条非环的边 } e \text{ 关联,}\\ 2 & \text{如果 } e \text{ 是环, } e \text{ 与 } x \text{ 关联,}\\ 0 & \text{如果 } x \text{ 不与 } e \text{ 关联.}\end{cases}$$

下面以二元域 $\mathbb{F}_2$ 为例，于是环实质上对应全零的列. 其他的列中每列包含两个 1，$N$ 的所有行的和模 2 是零向量.

我们考虑图 $G$ 的码 $\mathcal{C}(G)$，这是由关联矩阵 $N(G)$ 生成的二元码. 一个图 $H$ 是图 $G$ 的惠特尼(Whitney)对偶，如果 $E(G)=E(H)$ 且 $G$ 的码 $\mathcal{C}(G)$ 等于 $H$ 的对偶码 $\mathcal{C}(H)^{\perp}$. 显然，$H$ 是 $G$ 的一个惠特尼对偶当且仅当 $G$ 是 $H$ 的一个惠特尼对偶. 这个定义要求 $G$ 和 $H$ 有相同的边集，这在记号上是方便的. 但是，非正式地只需 $G$ 和 $H$ 的边由同一个集合标号，否则设置一个一一对应.

注意，有 $n$ 条边的一个多边形的码由长度为 $n$ 的所有偶重量的字组成；有 $n$ 条边的一个键图的码由两个常字组成. 一棵树的码由所有的字组成；余树的码仅由零字组成.

在图论中，一些术语以多种意义用在不同的上下文中. 在本章，我们用图 $G$ 的“圈”、“回路”、“割集”和“键”表示边集 $E(G)$ 的特定子集，如下所述. 读者所知的这些术语的其他用法现在暂时要忘掉.

如在第 20 章中，用码字 $\mathbf{x}$ 的支撑这个术语表示指标集的子集，即 $\mathbf{x}$ 中的非零的坐标．对二元码，可以把码字等同于它们的支撑．在$\mathcal{C}(G)$中字的支撑称为 $G$ 的割集；在$\mathcal{C}(G)^{\perp}$中字的支撑称为 $G$ 的圈．术语回路和键分别用于最小的非空圈和割集．用圈空间和割集空间分别表示所有圈的集合和所有割集的集合．当然，这些是域$\mathbb{F}_2$上的向量空间，其上两个集合相加等于它们的对称差．

475

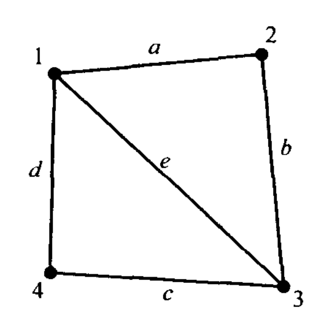
理解何时一个子集 $S\subseteq E(G)$是圈或割集是很容易的．关联矩阵中，由 $X$ 中的顶点指示的行之和(模 2)等于边集$\times(X, Y)$的支撑，其中$\times(X, Y)$的边从 $X$"跨过"$Y:=V(G)\setminus X$，即一端在 $X$ 且另一端在 $Y$ 的边．这就是，$S$ 是一个割集，当且仅当对某个 $X$，$Y$，$S=\times(X, Y)$．我们仅在 $X$ 和 $Y$ 划分顶点集时才用这个记号；允许 $X$ 或 $Y$ 为空集，此时 $S$ 为空集．

具有支撑 $S$ 的一个向量，比如说，在$\mathbb{F}_2$上正交于由顶点 $x$ 指示的 $N$ 的行，当且仅当 $x$ 与 $S$ 中的偶数条边相关联，环被计数两次．于是圈是 $E(G)$中使得每个顶点在 $G:S$ 中有偶数度的那些子集，$G:S$ 是 $G$ 中边集 $S$ 的生成子图．

**例 34.1** 考虑如下的图 $G$.

$G$ 的关联矩阵是

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}.$$




$G$ 中有四个圈：$\varnothing$，$\{a, b, e\}$，$\{c, d, e\}$和$\{a, b, c, d\}$．后三个事实上是回路．有 8 个割集．集合$\{a, b, c, d\}$既是一个圈又是一个割集；它是第 2 行和第 4 行的和的支撑．但是，$\{a, b, c, d\}$不是一个键；它包含较小的割集，例如，第 2 行的支撑$\{a, b\}$．集合$\{a, b\}$是一个键．键的另一个例子是$\{b, d, e\}$；它是第 1 行和第 2 行或第 3 行和第 4 行的支撑．

476

**问题 34A** (i)设 $G$ 为连通的．证明一个等价的叙述：$G$ 的割集数恰好是 $2^{|V(G)|-1}$；$G$ 的割集空间的维数是 $|V(G)|-1$.

(ii)证明：一般地，$G$ 的割集空间的维数为 $|V(G)|-|C(G)|$，这里 $C(G)$是 $G$ 的分支的集合．(作为一个推论，圈空间的维数是 $|E(G)|-|V(G)|+|C(G)|$.)

**例 34.2** $K_6$ 的圈空间和彼得森图的圈空间分别是维数为 10 和 6 且长度为 15 的二元码．(下一章的图 35.1 将显示 $K_6$ 是彼得森图相对于实射影平面上的一个嵌入的对偶，但它们不是惠特尼对偶，因为它们的码和维数大于边的数目.)这些码的最小距离分别为 3 和 5．我们说全幺的向量可以增加到这两个码的生成集中，在两种情形中，最小距离仍为 3 和 5，而维数增加 1.

**定理 34.1** 设 $G$ 为一个图.

(i)一个集合 $S\subseteq E(G)$ 是回路，当且仅当它是 $G$ 的一个多边形子图的边集.

(ii)假设 $G$ 是连通的. 一个割集 $\times(X, Y)$ 是 $G$ 的键，当且仅当由 $X$ 和 $Y$ 导出的 $G$ 的子图都是连通的.

**证明** 显然一个多边形的边集是最小的非空圈. 一个非空圈当然不是一个森林的边集(因为每棵树有一价的顶点)，因此包含一个多边形的边集；所以一个最小的非空圈是一个多边形的边集.

设 $S=\times(X, Y)$. 如果由 $X$ 和 $Y$ 导出的子图是连通的，则 $S$ 不能真正地包含一个非空的割集，因为在 $S$ 中删去边的任意真子集不会产生一个不连通图. 比如说，由 $Y$ 导出的子图是不连通的，存在 $Y$ 分成子集 $Y_1$ 和 $Y_2$ 的一个划分且它们之间没有边. 则 $S':=\times(X\cup Y_1, Y_2)$ 包含在 $S$ 中. 连通性蕴涵在 $X$ 和 $Y_1$ 之间，以及在 $X$ 和 $Y_2$ 之间存在边，这意味着 $S'$ 既是非空的又是 $S$ 的一个真子集. ■

477

读者可以验证，任意图 $G$ 的边的一个集合是 $G$ 的一个键，当且仅当它是 $G$ 的一个分支的键. 注意图 $G$ 的边的一个子集 $S$ 是 $G$ 的一个键，当且仅当删去 $S$ 中的边产生的图，其分支数比 $G$ 多(例如，开始时 $G$ 是连通的，得到一个不连通的图)且 $S$ 相对于这个性质是最小的.

给定图 $G$ 的边的一个集合 $S$，$S$ 是一个回路当且仅当删去不在 $S$ 中的边(以及由此产生的孤立点)得到一个多边形；$S$ 是一个键，当且仅当收缩不在 $S$ 中的边(并删去由此产生的孤立点)得到一个键图.

注意，图 $G$ 的一个与顶点 $x$ 关联且不包括环的边的子集 $S(x)$，总是一个割集. 这些割集生成割集空间——它们是关联矩阵的行的支撑. 根据定理 34.1(ii)，对每个 $x\in V(G)$，$S(x)$ 是键当且仅当 $G$ 是 2-连通的(或者是一个有两个顶点的连通图).

**问题 34B** 证明一个图的回路生成它的圈空间，且图的键张成它的割集空间. 为了做到这一点，仅需验证在一个二元线性码$\mathcal{C}$中的非零码字(在所有的非零码字支撑中，其支撑是最小的)生成这个码.(这对任意域上的线性码为真.)因此当 $G$ 的回路恰是 $H$ 的键，或者当 $G$ 的键恰是 $H$ 的回路时，$G$ 和 $H$ 是惠特尼对偶.

**例 34.3** 在图 34.2 中，由每张表描述的两个图是惠特尼对偶. 这是因为每对由平面对偶构成(见下面的定理 34.2). 例如，$\{a, e, g, c\}$ 和 $\{a, j, b\}$ 在立方体 $G$ 中是键且在 $G^*$ 中是回路；集合 $\{a, b, c, d\}$ 在 $G$ 中是回路且在 $G^*$ 中是键.

478

**问题 34C** 设 $G$ 和 $H$ 是满足 $E(G)=E(H)=E$ 的惠特尼对偶. 对任意的 $e\in E$，解释为什么 $G'_e$ 和 $H''_e$ 是惠特尼对偶.

**问题 34D** 设 $G$ 和 $H$ 是满足 $E(G)=E(H)=E$ 的惠特尼对偶，它们都是连通的. 证明在 $G$ 中 $S$ 是 $G$ 的支撑树的边集当且仅当 $E\setminus S$ 在 $H$ 中是 $H$ 的支撑树的边集.

**定理 34.2** 一个图 $G$ 是平面图，当且仅当它有一个惠特尼对偶. $G$ 的相对于 $G$ 的任意平面图示的对偶 $G^*$ 是 $G$ 的一个惠特尼对偶.

我们现在只证明第二部分(它蕴涵第一部分的“仅当”)，另一部分的证明推迟到本章的最后.

**证明** 设 $G^*$ 是 $G$ 的相对于 $G$ 的一个平面图示的对偶.

设 $S$ 为 $G$ 的一个回路. 于是 $S$ 是那个图示中 $G$ 的一个多边形子图 $P$ 的边集，由若尔当曲线定理，$S$ 把球或平面分为两部分；设 $\mathcal{F}_1$ 是向内的面的集合，$\mathcal{F}_2$ 是向外的面的集合. 这是 $G^*$ 的顶点的一个划分. 显然，$P$ 的每一条边与 $\mathcal{F}_1$ 的一个面关联，也与 $\mathcal{F}_2$ 的一个面关联. $G$ 的其他任意一条边位于(其端点可能除外)两部分之一中，因此只与 $\mathcal{F}_1$ 或 $\mathcal{F}_2$ 的成员关联. 总之，$S=\times(\mathcal{F}_1, \mathcal{F}_2)$ 是 $G^*$ 中的一个割集. 回路生成 $G$ 的圈空间，因此我们已经证明了 $G$ 的圈空间包含在 $G^*$ 的割集空间中.

现在我们注意到这个事实，对任意曲面上的一个嵌入，$G^*$ 的割集空间包含在 $G$ 的圈空间中. 对于一个给定的顶点关联的边，存在一个循环顺序(环出现两次). 划分 $G^*$ (区域或面)的顶点——比如说将它们染成红色和蓝色，并考虑 $G^*$ 的由与一个红色区域和一个蓝色区域关联的边组成的割集 $C$. 与 $G$ 的一个顶点关联的 $C$ 的边的数目必定是偶数，见图 34.6. (这等价于说将一个多边形的顶点染成红色和蓝色，则端点颜色不同的边的数目是偶数.)因此 $C$ 是 $G$ 中的一个圈.

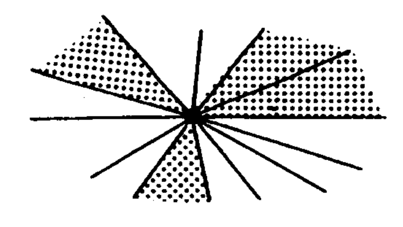


图 34.6

479

于是，$G$ 的圈空间等于 $G^*$ 的割集空间. ■

欧拉公式是到目前为止已证明的结果的一个推论. 问题 34A 说 $G$ 的圈空间的维数是 $|E(G)|-(|V(G)|-|C(G)|)$，同时 $G^*$ 的割集空间的维数是 $|F(G)|-1$(我们已经提及 $G^*$ 总是连通的). 当我们使这两个式子相等时，得到(33.2).

惠特尼定理使得下面的 S. MacLane(1937)定理有一个紧凑的证明.

**定理 34.3** *一个图 $G$ 是平面的，当且仅当 $G$ 的圈空间有一组基 $\mathcal{B}=\{B_1, B_2, \cdots, B_k\}$ 使得 $G$ 的每一条边出现在 $\mathcal{B}$ 的至多两个成员中.*

**证明** 如果 $G$ 是平面的，除一个面之外，所有面的边界提供这样一组基. 这是因为，如果 $G^*$ 是 $G$ 在一个平面上相对于某个嵌入的对偶，由于 $G^*$ 是连通的，则与 $G^*$ 的除一个点之外的所有其他点($G$ 的面)关联的所有非环边的集合为 $G^*$ 的割集空间($G$ 的圈空间)提供了一组基，且每条边是其中至多两个集合的一个元素.

现在假设 $G$ 的圈空间有一组如定理陈述中那样的基. 设 $B_0=B_1+B_2+\cdots+B_k$. $G$ 的任意一条边在 0 或 2 个 $B_i$ 中，$0\leqslant i\leqslant k$. 定义一个图 $H$，它的顶点是 $0, 1, \cdots, k$，它的边集是 $E(G)$，当 $e$ 在 $B_i$ 的两个集合中时，它与 $H$ 中的两个整数 $j$ 和 $\ell$ 关联，使得 $e\in B_j$ 且 $e\in B_\ell$；当 $e$ 不在任何一个集合 $B_i$ 中时，$e$ 是 $H$ 的一个环(在任意顶点 $i$). 我们断言 $H$ 是 $G$ 的惠特尼对偶.

480

在 $H$ 中与顶点 $i$ 关联的 $H$ 中的非环边的集合是 $B_i$，这当然是 $H$ 的一个割集. 因为这些 $B_i$ 生成 $G$ 的圈，所以 $G$ 的圈空间包含在 $H$ 的割集空间中. 但我们知道 $G$ 的圈空间的维数为 $k$，同时 $H$ 的割集空间的维数 $\leqslant k$，因为 $H$ 有 $k+1$ 个顶点. 得出结论：$G$ 的圈空间等于 $H$ 的割集空间，即它们是惠特尼对偶. 因此由定理 34.2，$G$ 是平面的. ■

如所承诺的，现在我们应用惠特尼对偶(而没有参照平面或球)给出一些平面图的结果及它们的对偶的结果.

**定理 34.4** 如果 $G$ 和 $H$ 是惠特尼对偶且 $H$ 是连通的，则 $G$ 是二部图当且仅当 $H$ 是欧拉图(有一个欧拉回路).

**证明** $G$ 是二部图当且仅当整个边集 $E(G)$ 是 $G$ 的一个割集. 因为 $G^*$ 是连通的，它是欧拉图当且仅当 $E(G)$ 是 $G^*$ 的一个圈；见定理 1.2. 这两个条件是等价的，因为 $G^*$ 是 $G$ 的一个惠特尼对偶. ■

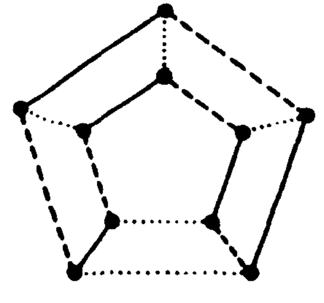


图 34.7

一个三价图的 Tait 染色(由英国数学家 P. G. Tait 得名)是其边用三种颜色染色，颜色比如说是 $\alpha$，$\beta$ 和 $\gamma$，使得每种颜色出现在每一个顶点. 图 34.7 显示了这样的染色. 一个三价图的 Tait 染色的存在性等价于其边划分为三个完美匹配(参见第 5 章)，因此由问题 5A，一个二部的三价图有 Tait 染色.

**定理 34.5** 如果 $G$ 和 $H$ 是惠特尼对偶且 $G$ 是三价的，则 $G$ 有 Tait 染色当且仅当 $H$ 是 4-可染色的.

481

**证明** 我们断言一个三价图 $G$ 有 Tait 染色，当且仅当在 $G$ 中存在两个圈 $S_1$ 和 $S_2$ 使得 $E(G)=S_1\cup S_2$. 给定染色，取 $S_1$ 为染 $\alpha$ 和 $\gamma$ 的边的并，$S_2$ 为染 $\beta$ 和 $\gamma$ 的边的并. $S_1$ 和 $S_2$ 都是圈，因为每个顶点与 $S_1$ 中的两条边和 $S_2$ 中的两条边关联. 反之，如果 $E(G)$ 是两个圈 $S_1$ 和 $S_2$ 的并，用颜色

$$\begin{cases}\alpha & \text{如果 } e\in S_1, e\notin S_2,\\ \beta & \text{如果 } e\notin S_1, e\in S_2,\\ \gamma & \text{如果 } e\in S_1\cap S_2\end{cases}$$

染边 $e$. 每个顶点 $x$ 在边集为 $S_1$ 及 $S_2$ 的生成子图中有偶数的度(在 0 和 3 之间)；但 $E(G)=S_1\cup S_2$ 蕴涵 $x$ 在 $S_1$ 和 $S_2$ 的生成子图中的度都是 2，而且每种颜色有一条边与 $x$ 关联.

第二个断言是 $H$ 有正常的 4-染色，当且仅当 $E(H)$ 可以表示为 $H$ 的两个割集的并. 如果 $E(H)$ 是 $\times(X_1, X_2)$ 和 $\times(Y_1, Y_2)$ 的并，则 $X_1\cap Y_1$，$X_1\cap Y_2$，$X_2\cap Y_1$，$X_2\cap Y_2$ 是一个正常 4-染色的颜色类. 如果 $A$，$B$，$C$，$D$ 是一个正常 4-染色的颜色类，则 $E(H)$ 是 $\times(A\cup B, C\cup D)$ 和 $\times(A\cup C, B\cup D)$ 的并.

根据这两个观察和惠特尼对偶的定义，完成定理的证明. ■

一个图的割边是删去这条边使图的分支数增加的边(即如果图原来是连通的，则变成不连通的). 这是环的对偶概念. 一条割边是满足单元素集 $\{e\}$ 是割集的一条边 $e$；一个环是满足单元素集 $\{e\}$ 是一个圈的一条边 $e$. (一些作者用非圈边表示割边，因为它是不包含在回路中的边. 也有用术语桥的.)

**问题 34E** 证明有一条割边的三价图没有 Tait 染色.

根据四色定理，每个没有割边的三价平面图有 Tait 染色. (在 $G$ 中，一条割边在其对偶中是一个环，因而没有正常的染色.)平面性是必需的，因为彼得森图是无割边的三价图但没有 Tait 染色是一个例子.

482

反之，我们断言，为了证明四色定理，建立每个无割边的三价平面图有 Tait 染色就够了. 这是因为，假设每个无割边的三价平面图 $G$ 的区域能被正常地 4-染色. 那么，给定一个平面

图 G，对每个度$\neq 3$的顶点 $x$，用图 34.8 中指示的 5 度顶点的构形代替.（甚至对度为 1 和 2 的顶点也可以这样做.）由此产生更多的区域(在对偶 $G^*$ 中更多的顶点)，但保持原来区域的相邻性，于是，如果这个较大的三价图的区域是 4-可染色的，那么我们就得到了原图的染色. 由定理 34.5，较大的三价图的区域是 4-可染色的，当且仅当它有 Tait 染色.

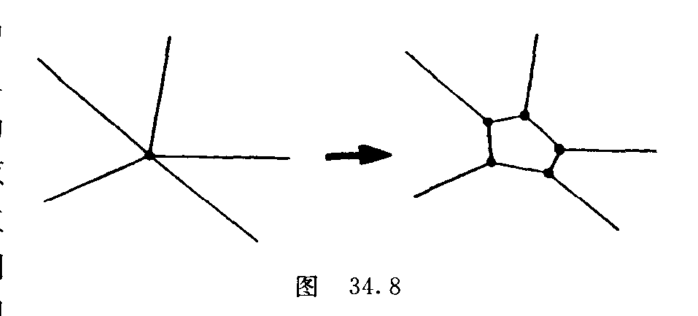


图 34.8

Tait 在 1880 年猜测每个 3-连通的平面三价图有一个哈密顿回路，这蕴涵着这种图有 Tait 染色. W. T. Tutte(1956)发现了一个反例并证明每个 4-连通的平面三价图有哈密顿回路.

**定理 34.6** *如果 $G$ 和 $H$ 是没有孤立顶点的惠特尼对偶且 $G$ 是不可分的，则 $H$ 是不可分的.*

**证明** 定理 32.2 证明 $G$ 的任意两条边包含在 $G$ 的一个回路中. 因此 $H$ 的任意两条边包含在 $H$ 的一个键中. 如果两条边 $a$ 和 $b$ 包含在一个键$\times(X, Y)$中，则在由 $X$ 导出的子图中可以找到连结 $a$ 的一个端点和 $b$ 的一个端点的一条简单路，以及在由 $Y$ 导出的子图中连结另两个端点的一条简单路，并找到包含 $a$ 和 $b$ 的一个多边形. 因此，$H$ 的任意两条边包含在 $H$ 的一个回路中. 这蕴涵着 $H$ 是不可分的. ■

483

**推论** *在一个不可分图 $G$(不是连杆图)的平面嵌入中，与一个面关联的边是 $G$ 的一个回路.*

**证明** 与 $G$ 的一个面关联的边集 $S$ 是 $G^*$ 中与一个顶点关联的边的集合. 但由定理 34.5，$G^*$ 是不可分的，因此 $S$ 在 $G^*$ 中是一个键. 则 $S$ 是 $G$ 中的一个回路. ■

**问题 34F** 连通图 $G$ 的两条边 $a$ 和 $b$ 都包含在 $G$ 的一个回路中，它们也包含在 $G$ 的一个键中.

**定理 34.7** *设没有孤立顶点的简单图 $G$ 和 $H$ 是惠特尼对偶. 如果 $G$ 是 3-连通的，则 $H$ 也是 3-连通的.*

**证明** 假设 $G$ 是 3-连通的. 对 $x\in V(G)$，设 $S(x)$表示与 $x$ 关联的边集. 每个集合 $S(x)$ 是一个键，该键具有性质 $G'_{S(x)}$ 是不可分的，由定义，这些键生成 $G$ 的割集空间.

因此在 $H$ 中，存在回路的一个族$\mathcal{F}$，回路生成 $H$ 的圈空间，这里$\mathcal{F}$的每个成员 $S$ 是一个回路，它有性质 $H''_S$ 是不可分的.

我们知道 $H$ 是不可分的；作相反的假设，它不是 3-连通的. 则 $H$ 是 $H$ 的两个子图 $A$ 和 $B$ 的边不交的并，每个子图至少有两条边，且这里 $A\cap B$ 由两个孤立的顶点构成，比如说 $x$ 和 $y$. 在 $H$ 中，如果一个多边形既包含 $A$ 的边又包含 $B$ 的边，则在它的顶点中一定有 $x$ 和 $y$. 如果这样一个多边形被收缩，会得到一个可分图，因为它是由在 $A$ 和 $B$ 中分别收缩多边形的边(这会使 $x$ 和 $y$ 重合)得到的图的并；以多边形顶点的等同得到的顶点是这两个收缩子图的唯一一个公共顶点(读者可以验证在每个收缩过的图中仍至少剩下一条边).

484

于是，$\mathcal{F}$ 中的回路完全包含在 $E(A)$或 $E(B)$中. 设 $C$ 是 $H$ 的任意一个回路. 因为$\mathcal{F}$生成 $H$ 的圈空间，所以 $C\cap E(A)$和 $C\cap E(B)$分别是包含在 $E(A)$和 $E(B)$中的$\mathcal{F}$的成员的模 2 和.

因此$C\cap E(A)$和$C\cap E(B)$都是圈，并且$C$的极小性蕴涵$C\cap E(A)$或$C\cap E(B)$是空的．由此得出$H$中的每个回路或者包含在$E(A)$中，或者包含在$E(B)$中，这与$H$的不可分性矛盾． ■

**问题 34G** (i)设$G$是简单的3-连通图且$S$是$G$的一个键．证明$G'_S$是不可分的，当且仅当$S$等于$S(x)$，这里$S(x)$是与$G$的一个顶点$x$关联的边集．

(ii)证明：如果$G$和$H$是有等价码的简单3-连通图，则$G$与$H$同构．

**定理 34.8** 设$G$是嵌入在球上的简单3-连通图．$G$的一个回路$C$是与这个嵌入中的一个面关联的边集，当且仅当$G''_C$是不可分的．

**证明** 回路$C$是与一个面关联的边集，当且仅当在对偶$H:=G^*$中它是与一个顶点关联的边集．由问题34G(i)，这种情形出现，当且仅当$H'_C$是不可分的．后一个图是$G''_C$的惠特尼对偶． ■

因此，在简单3-连通平面图的嵌入中，面的边界构成的多边形是唯一确定的．一般地，这对不可分图不真——见图34.5．如果知道面，即围绕面的回路，嵌入就确定了(这在下一章稍加解释)，而且有下面的结果．

**推论** 一个简单的3-连通图在球上有唯一的嵌入．

**例 34.4** 如果$K_5$是平面的，没有一个四边形会是一个面，因为四边形四个边的收缩产生一个有两个顶点、四个连杆及其中一个顶点有两个环的图，且这个图不是不可分的．另一方面，一个三角形必定是一个面． [485]

我们还可以得到简单的3-连通图$K_5$、$K_{3,3}$和彼得森图不是平面图的另一个证明：分别收缩$K_5$中的任意一个三边形、$K_{3,3}$中的任意一个四边形和彼得森图中的任意一个五边形的边，总产生一个不可分图．于是按照定理34.8，如果这些图是平面的，每个三边形、四边形和五边形都是嵌入中一个面的边界．但在相应的图中，每条边分别属于3个三边形、4个四边形和4个五边形，与平面性矛盾．

E. Steinitz(1922)刻画了3维凸多面体的图的性质．

**定理 34.9** 图$G$是一个3维凸多面体的图，当且仅当$G$是简单的、平面的和3-连通的．

3维多面体的图是3连通的是定理32.5的特殊情形．在这里我们不证明定理的其余部分．

对定理34.2的"当"部分，我们需要一个引理．

**引理 34.10** 设$G$和$H$是有相同边集$E$的图．假设$G$是边不交的子图$G_1$和$G_2$的并，使得$|V(G_1)\cap V(G_2)|\leqslant 1$．设$H$的子图$H_1$和$H_2$分别有边集$E(G_1)$和$E(G_2)$，孤立顶点已删去．

(i)如果$G$和$H$是惠特尼对偶，则$G_i$和$H_i$对$i=1$和$i=2$都是惠特尼对偶．

(ii)如果$G_i$和$H_i$对$i=1$和$i=2$都是惠特尼对偶且$|V(H_1)\cap V(H_2)|\leqslant 1$，则$G$和$H$是惠特尼对偶．

**证明** 由定理34.1，容易看出$G$的每一个键都完全包含在$E(G_1)$中或$E(G_2)$中．此外，子集$S\subseteq E(G_i)$是$G_i$的一个键，当且仅当它是$G$的一个键．

假设$G$和$H$是惠特尼对偶．如果$S$是$G_i$的一个键，则$S$是包含在$E(H_i)$中的$H$的一个回路，于是$S$是$H_i$的一个回路．而且如果$S$是$H_i$的一个回路，则它是$H$的一个回路．因此

它是 $G$ 的包含在 $E(G_i)$ 中的一个键，从而是 $G_i$ 的键.

假设 $G_i$ 和 $H_i$ 对 $i=1$，2 是惠特尼对偶且 $|V(H_1)\cap V(H_2)|\leqslant 1$. 设 $S$ 是 $G$ 的一个键. 则 $S$ 是 $G_1$ 或 $G_2$ 的键，于是 $S$ 或者是 $H_1$ 或者是 $H_2$ 的回路. 那么 $S$ 确实在 $H$ 中是一个回路. 如果 $S$ 是 $H$ 的一个回路，则它或者是 $H_1$ 或者是 $H_2$ 的回路. 于是它是 $G_1$ 或 $G_2$ 的一个键，且因此它是 $G$ 的键. ■

486

**定理 34.2 的证明(续)** 为了给出该定理剩下部分的证明，首先建立如下的断言. 给定边集相同($E$)且没有孤立顶点的一对惠特尼对偶 $G$，$H$，我们断言存在一个可能不同的惠特尼对偶 $H^0$，$H^0$ 有一组称之为关于 $G$ 的步路. 即 $H^0$ 中的步路 $w_x$ 的族 $\{w_x: x\in V(G)\}$，对 $G$ 的每个顶点 $x$，使得 $w_x$ 在 $H^0$ 中恰好穿过 $G$ 中与 $x$ 关联的边，穿过环两次、非环边一次. 对边数用归纳法. 假定 $G$ 没有孤立顶点.

首先注意，当 $G$ 不可分时断言易于证明. 当然，断言对环图成立. 否则没有环且对每个顶点 $x$，在 $G$ 中与 $x$ 关联的边集 $S(x)$ 在 $G$ 中是一个键，因此在 $H$ 中是一个回路. 我们只需设 $w_x$ 为 $H$ 中的一条简单闭路，它穿过 $H$ 中的环路 $S(x)$ 的边.

如果 $G$ 不是不可分的，存在边不交的子图 $G_1$ 和 $G_2$，每个子图中至少有一条边且它们没有公共顶点或者有一个公共顶点，使得 $G_1$ 和 $G_2$ 的并是 $G$. 如同引理 34.10 中给定 $H_1$ 和 $H_2$，$H_i$ 是 $G_i$ 的惠特尼对偶，$i=1$，2. 由归纳假设，存在图 $H_i^0$，它们是 $G_i$ 的惠特尼对偶且对 $G_i$ 有步路系 $\{w_x^{(i)}: x\in V(G_i)\}$，$i=1$，2. 我们可以取 $H_1^0$ 和 $H_2^0$ 是顶点不相交的. 如果 $G_1$ 和 $G_2$ 不相交，设 $H^0$ 是 $H_1^0$ 和 $H_2^0$ 的不相交的并；那么两个步路系的并为 $G$ 提供了一个步路系. 如果 $G_1$ 和 $G_2$ 有一个公共顶点 $z$，在 $H_1^0$ 和 $H_2^0$ 中分别有步路 $w_z^{(1)}$ 和 $w_z^{(2)}$ 穿过 $G_1$ 和 $G_2$ 中与 $z$ 关联的边. 设 $H^0$ 作为 $H_1^0$ 和 $H_2^0$ 的并得到，但是在 $H_1^0$ 中的步路 $w_z^{(1)}$ 上的某个点等同于在 $H_2^0$ 中的步路 $w_z^{(2)}$ 上的某个点. 我们把这两个步路结合为一个，它穿过 $G$ 中与 $z$ 关联的边；这条步路与 $H_1$ 和 $H_2$ 的步路系中剩下的步路一起为 $G$ 提供了一个步路系. 在任一种情况下，由引理 34.10，$H^0$ 是 $G$ 的惠特尼对偶.

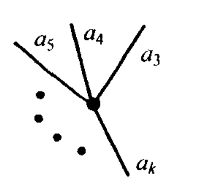
487

最后，我们证明下面的内容. 设 $G$ 是有惠特尼对偶 $H$ 的图；对于 $G$，$H$ 有一个步路系 $\{w_x: x\in V(G)\}$. 我们断言在球上 $G$ 有一个嵌入，使得 $G$ 中与 $x$ 关联的边按照它们在步路 $w_x$ 中出现的同一循环顺序出现. 我们对边的数目用归纳法进行证明.

如果 $G$ 仅有环，则 $H$ 是森林. 设 $e$ 是 $G$ 中的一个环使得 $e$ 在 $H$ 中与一价顶点关联. 设 $z$ 是 $G$ 中与 $e$ 关联的顶点. 在 $H$ 中 $w_z$ 显然连续两次穿过 $e$，比如说

$$w_z=(s_0,e,s_1,e,s_2=s_0,a_3,s_3,a_4,s_4,\cdots,a_k,s_0),$$

这里 $s_i$ 是 $H$ 的顶点. 图 $G'_e$ 和 $H''_e$ 是惠特尼对偶，在 $w_z$ 中取消 $e$ 将在 $H''_e$ 中为 $G'_e$ 提供一个步路系，因此由归纳假设，$G'_e$ 有一个平面图示，使得 $G'_e$ 中与 $z$ 关联的边按照它们在取消 $e$ 的步路 $w_x$ 中出现的同一循环顺序出现. 在嵌入中表示 $z$ 的点的一个小邻域内，可以插入环 $e$ 以得到所要的 $G$ 的嵌入(见图 34.9).



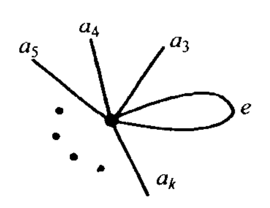



图 34.9

现在设 $e$ 在 $G$ 中是端点为 $y$ 和 $z$ 的非环边．则 $G''_e$ 和 $H'_e$ 是惠特尼对偶，且我们断言在 $H'_e$ 中有 $G''_e$ 的一个自然的步路系 $\{u_x: x\in V(G''_e)\}$．对 $x\neq y$，$z$，取 $u_x:=w_x$．对由等同 $y$ 和 $z$ 得到的新顶点 $x_0$，结合 $w_y$ 和 $w_z$ 并舍去 $e$ 如下．比如说

488

$$w_y=(s_0,e,s_1,a_2,s_2,\cdots,s_{k-1},a_k,s_0)$$

且

$$w_z=(t_0,e,t_1,b_2,t_2,\cdots,t_{m-1},b_m,t_0),$$

这里 $e$，$a_2$，$a_3$，…，$a_k$ 和 $e$，$b_2$，$b_3$，…，$b_m$ 在 $G$ 中分别是与 $y$ 和 $z$ 关联的边(环出现两次)，且 $s_i$ 和 $t_j$ 是 $H$ 的顶点．如果必要，反转其中一条步路，可以假设 $s_0=t_0$ 且 $s_1=t_1$．然后取

$$u_{x0}:=(s_1,a_2,s_2,\cdots,s_{k-1},a_k,s_0,b_m,t_{m-1},b_{m-1},\cdots,b_3,t_2,b_2,s_1).$$

由归纳假设，在平面上 $G''_e$ 有一个嵌入使得 $G''_e$ 中与 $x$ 关联的边按照它们在步路 $u_x$ 上出现的同一循环顺序出现．在嵌入中表示 $x_0$ 的点的小邻域内，可以"恢复收缩的"$e$ 以得到所需的 $G$ 的嵌入(见图 34.10)． ■

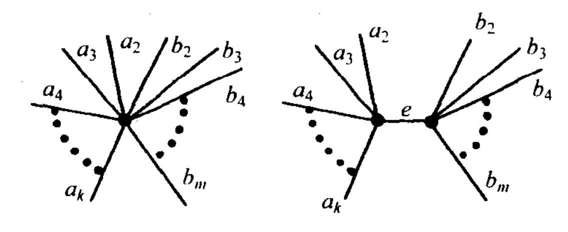


图 34.10

**问题 34H** 在至少有 $2k-2$ 条边的一个 $k$-塔特连通图(定义见问题 32D)中，每个环路和每个键至少包含 $k$ 条边．

**问题 34I** 一个拟阵由一个集合 $X$(这里我们假定它是有限的)和称为回路的非空子集的一个族 $\mathcal{C}$ 构成，使得 $\mathcal{C}$ 中没有一个回路是另一个回路的真子集，并且如果 $A$，$B\in\mathcal{C}$，$x\in A\cap B$，$y\in A\setminus B$，则存在 $C\in\mathcal{C}$ 使得 $C\subseteq A\cup B$，$y\in C$，$x\notin C$．后一个性质称为"消灭公理"．

(i)证明一个有限图的边集与它的所有回路(多边形的边集)合在一起是一个拟阵．

(ii)证明在任何一个域上的线性码中，码字的最小非空支撑的族可为一个拟阵提供回路．

489

(iii)设 $(X,\mathcal{F})$ 是如同第 23 章定义的一个组合几何，设 $\mathcal{C}$ 是 $X$ 的最小独立子集的族，证明 $(X,\mathcal{C})$ 是一个拟阵．

(在处理这个问题的所有部分时，先做(iii)并从它导出其他结果可节省工作量．)

## 评注

惠特尼(Hassler Whitney，1907—1989)是哈佛大学教授，后任普林斯顿高等研究院教授，是拓扑学的先驱之一，在生命的最后二十年，他非常关注数学教育．1982 年他获得沃尔夫(Wolf)奖．惠特尼从耶鲁获得了音乐学位，他演奏小提琴、中提琴和钢琴，是普林斯顿社区管弦乐队的首席小提琴手．

拟阵由惠特尼(Hassler Whitney)在 1935 年引入，目的是抽取线性无关性、图中的环路和键以及对偶的特定性质．它们的理论对几何格的理论是"隐形的"．见 Welsh(1976)和 Crapo and Rota(1971)．

## 参考文献

H. Crapo and G.-C. Rota (1971), *On the Foundations of Combinatorial Theory: Combinatorial Geometries*, M. I. T. Press.

S. MacLane (1937), A structural characterization of planar combinatorial graphs, *Duke math. J.* **3**, 460–472.

P. G. Tait (1880), Remarks on the colouring of maps, *Proc. Roy. Soc. Edinburgh* **10**, 501–503.

W. T. Tutte (1956), A theorem on planar graphs, *Trans. Amer. Math. Soc.* **82**, 99–116.

W. T. Tutte (1984), *Graph Theory*, Encylodpedia of Math. and its Appl. **21**, Addison-Wesley.

D. J. A. Welsh (1976), *Matroid Theory*, Academic Press.

H. Whitney (1932), Nonseparable and planar graphs, *Trans. Amer. Math. Soc.* **34**, 339–362.

H. Whitney (1935), On the abstract properties of linear dependence, *Amer. J. Math.* **57**, 509–533.

490

# 第35章　图在曲面上的嵌入

本章讨论图在球之外的曲面上的嵌入. 曲面的分类(见 Fréchet and Fan，1967)表明，在同胚意义上，曲面有两个无穷族. 用$\mathcal{T}_g(g>0)$表示亏格为$g$($g$-环面)的可定向曲面. 这可以看成是带$g$个"柄"或$g$个"洞"的球；$\mathcal{T}_0$是球. 用$\mathcal{N}_n(n\geqslant 1)$表示通过在球上插入$n$个"交叉帽"(这些不能嵌入在$\mathbb{R}^3$中)构造的不可定向曲面. 本章叙述欧拉公式的推广，证明见 Fréchet and Fan (1967)；或者对可定向的情形，见 Chartrand and Lesniak(1986).

**定理 35.1**　*对图$G$在$\mathcal{T}_g$上的2-胞腔嵌入，*

$$|F(G)|-|E(G)|+|V(G)|=2-2g.$$

*对一个连通图$G$在$\mathcal{N}_n$上的2-胞腔嵌入，*

$$|F(G)|-|E(G)|+|V(G)|=2-n.$$

*对任意的嵌入，不必是2-胞腔嵌入，在上面的等式中用"$\geqslant$"代替"$=$"得到的不等式成立.*

**例 35.1**　图35.1显示了彼得森图$P$在实射影平面$\mathcal{N}_1$上的嵌入. 在这个图示中，边界上的对径点是相同的. 其中有6个面，每个面都是五边形. 更精确些，相对于这个嵌入，$P$的对偶图是完全图$K_6$.

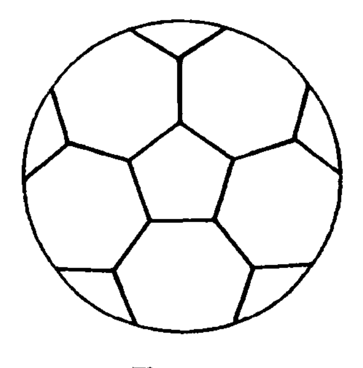


图　35.1

491

(这建立了$P$的15条边和$K_6$的15条边之间的奇怪的一一对应. 前面我们已经看到在$P$的10个顶点和$K_5$的10条边之间存在一个一一对应.)

(实射影平面可以视为球的曲面，这里对径点已被等同；彼得森图可以想象为正十二面体的图，这里对径点已被等同.)

**例 35.2**　图35.2显示了完全图$K_7$在环面$\mathcal{T}_1$上的一个嵌入. 我们利用环面通常的表示，这里水平边界和竖直边界被等同. 有14个三角形面. 相对于这个嵌入的对偶图有14个3度的顶点和7个六边形面，其中任意两个面是相邻的. 这是Heawood图(定义见第31章)，它作为环面上其面需要7种颜色的一个例子而给出.

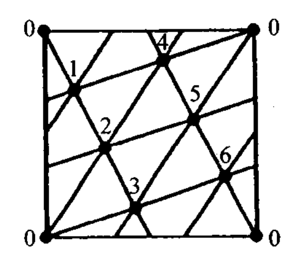



图　35.2

492

**定理 35.2**　*如果一个无环图$G$在$\mathcal{T}_g$上有一个嵌入，$g>0$，则*

$$\chi(G)\leqslant\frac{7+\sqrt{1+48g}}{2}.$$

**证明**　假设$G$被嵌入在$\mathcal{T}_g$上. 可以假设$G$是简单的、连通的且至少有3个点. 我们断言存在一个度至多为$N-1$的顶点$x$，这里$N:=(7+\sqrt{1+48g})/2$. 这个事实一旦建立，定理将由对点的数目进行归纳得到；因为如果这个点$x$被删去且剩下的图有正常的$\lfloor N\rfloor$-染色，则对$x$有一种空余的颜色.

由定理35.1，我们有

$$2-2g \leqslant f-e+v,$$

这里 $f := |F(G)|$，$e := |E(G)|$，$v := |V(G)|$. 因为每个面至少与三条边关联，$3f \leqslant 2e$. 设 $d$ 为 $G$ 的顶点的平均度. 作一个相反的假设，$d > N-1$. 这蕴涵 $v > N$. 对 $g \geqslant 1$，因为 $N \geqslant 7$，故 $d > 6$，而且我们有

$$2-2g \leqslant \frac{2}{3}e-e+v=-\frac{1}{3}e+v=-\frac{1}{6}vd+v=\frac{1}{6}v(6-d),$$

$$12g-12 \geqslant v(d-6) > N(N-7) = 12g-12.$$

这给出了所允诺的矛盾. ■

下面是从定理 35.2 得出的界的短表：

| 亏格 $g$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\chi \leqslant$ | 7 | 8 | 9 | 10 | 11 | 12 | 12 | 13 | 13 | 14 | 15 | 15 | 16 | 16 | 16 |

定理 35.2 的断言是最佳可能的结果，即对某个图在 $\mathcal{T}_g$ 上的嵌入需要 $\left\lfloor \frac{7+\sqrt{1+48g}}{2} \right\rfloor$ 种颜色，这以 Heawood 猜想而著称，直到它在 1968 年被 Ringel 和 Youngs 证明. 见 Ringel (1974). 他们证明的是下面更强的结果.

493

**定理 35.3**(Ringel-Youngs) *给定 $g \geqslant 0$，设*

$$n := \left\lfloor \frac{7+\sqrt{1+48g}}{2} \right\rfloor.$$

*则完全图 $K_n$ 可嵌入在 $\mathcal{T}_g$ 上.*

我们只证明这个结果的一小部分(见下面的定理 35.4). 例如，对图 $G$ 在 $\mathcal{T}_{20}$、$\mathcal{T}_{21}$ 和 $\mathcal{T}_{22}$ 上的嵌入，定理 35.3 表明 $\chi(G) \leqslant 19$. 定理 35.4 表明 $K_{19}$ 能嵌入在 $\mathcal{T}_{20}$(因此 $\mathcal{T}_{21}$ 和 $\mathcal{T}_{22}$)上，对 $g=20$，21，22 验证 Heawood 猜想.

我们需要用图论的术语组合地理解 2-胞腔嵌入. 这是重要的.

在一个曲面 $S$ 上给定图 $G$ 的一个 2-胞腔嵌入，可以经过任意一个面 $F$ 的边界在 $G$ 中得到一个闭步路 $w_F$. 起始点和方向都不重要. 在许多情形，这可能是 $G$ 中的一条简单闭步路，但当 $G$ 是一棵嵌入在球上的树时，有单一一个面且这个路径穿过每条边两次(见图 2.4). 一般地，每条边或者恰好属于 $\{w_F : F \in F(G)\}$ 中的两条步路，或者在 $\{w_F : F \in F(G)\}$ 的一条步路中出现两次. $G$ 中的闭步路系 $\mathcal{M}$ 具有 $G$ 的每条边在 $\mathcal{M}$ 的步路中出现两次的性质，$\mathcal{M}$ 称为 $G$ 中的一个网.

**例 35.3** 下面是 $K_5$ 中的两个网. 步路由它们的顶点序列描述：

$\mathcal{M}_1 = \{(1,2,3,4,5,1),(1,2,4,1),(2,3,5,2),(3,4,1,3),(4,5,2,4),(5,1,3,5)\}$,

$\mathcal{M}_2 = \{(1,2,4,5,1),(1,3,2,5,3,4,2,3,5,4,1),(1,4,3,1,5,2,1)\}$.

网 $\mathcal{M}_1$ 由简单的路径组成(一个五边形和五个三角形)，但 $\mathcal{M}_2$ 中的第二个步路穿过两条边两次.

一个三角网是由长度为 3 的简单闭路组成的网. 因此，对于 $K_n$，一个三角网等价于区组规模为 3 且指标为 2 的一个 2-设计 $S_2(2,3,n)$. 但是这些设计极少与曲面上 $K_n$ 的嵌入对应，

因为一个重要的附加条件必须成立.

494

在一个连通图 $G$ 中给定网 $\mathcal{M}$，我们试着构造一个曲面上 $G$ 的 2-胞腔嵌入，使得这些步路以 $G$ 的面为界. 其实别无选择，我们必须如下进行. 对长度为 $\ell$ 的每个步路 $w\in M$，需要一个对应的闭圆盘 $F_w$，例如在平面上的一个凸 $\ell$ 边形及其内部(甚至对 $\ell=1$ 和 2，尽管在这些情形我们不能用直线段作为边). 按照路径 $w$ 的顶点在 $w$ 中出现的顺序给 $F_w$ 的顶点和边标号. (因此，如果 $w$ 不是一条简单的闭路，$F_w$ 的一些顶点以及也许一些边会得到相同的标号.)将这些圆盘的边界"粘贴"或"缝合"在一起.

考虑所有圆盘 $F_w$ 的不交并. 对 $G$ 的每个顶点 $x$，等同用 $x$ 标号的所有点. 对 $G$ 的每条边，按照一对一的连续方式在由边的端点指示的方向上等同标号为 $e$ 的诸边的内部点. (承认环有两个方向是必需的.)

图 35.3 和图 35.4 分别显示了由例 35.3 的网中的步路的顶点标号的平面(圆盘)上的多边形区域. 在图 35.5 中，我们已经开始了对图 35.3 粘贴的过程，剩下要等同边界上的对径点(而且得到 $K_5$ 画在上面的实射影平面).

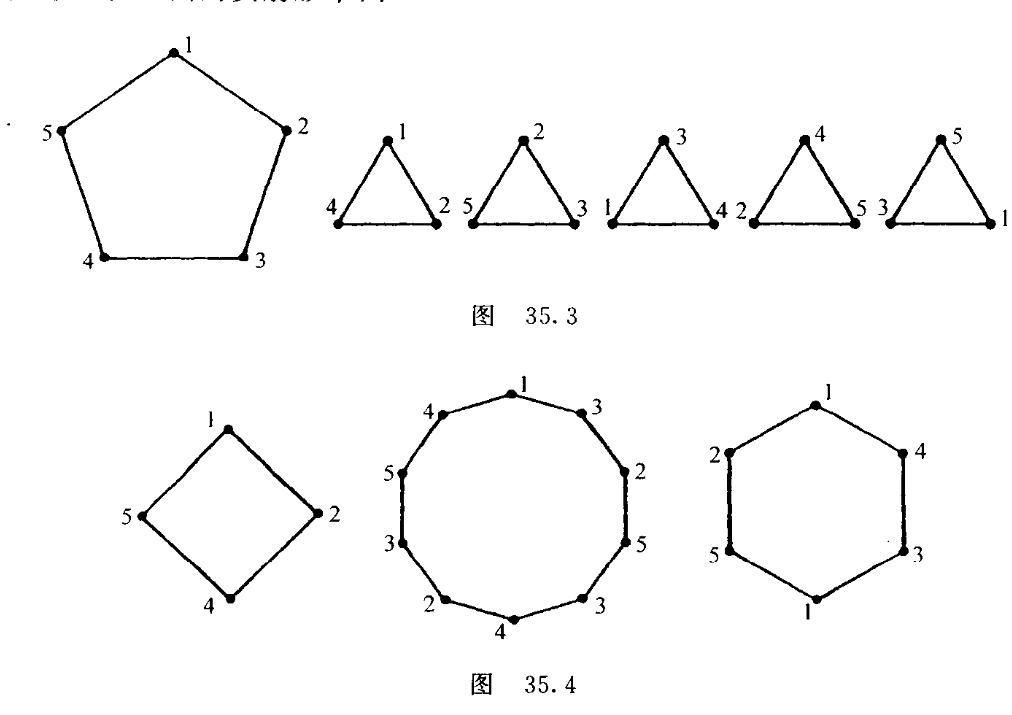



图 35.3



图 35.4

一般地，由这种粘贴构造的拓扑空间与围绕圆盘 $F_x$ 内部的点 $x$ 以及圆盘 $F_x$ 边界上一条边内部的点的开圆盘(2-胞腔)邻域同胚(因为每条边在网的两个步路中). 但在顶点会有麻烦，那里有许多圆盘 $F_w$ 相遇. 例如，假设在一个特定的网中经过顶点 $x$ 的步路有顶点序列

$$(\cdots,1,x,2,\cdots),(\cdots,2,x,3,\cdots),(\cdots,3,x,1,\cdots),$$
$$(\cdots,4,x,5,\cdots),(\cdots,5,x,6,\cdots),(\cdots,6,x,4,\cdots).$$

对应于前三条步路的圆盘合在一起组成 $x$ 的一个邻域，这是一个 2-胞腔，但和其他三个

圆盘一起，$x$ 的邻域看起来像两个在顶点接触的圆锥. 下面定义的图 $\mathcal{M}_x$ 在这种情形由两个不相交的三角形构成.

对一个顶点 $x \in V(G)$，考虑图 $\mathcal{M}_x$，这里 $V(\mathcal{M}_x)$是与 $x$ 关联的 $G$ 中的边集，$V(\mathcal{M}_x)$中的两个成员 $a$，$b$ 在 $\mathcal{M}_x$ 中是相邻的，若它们在 $\mathcal{M}$的某个步路中作为相继边出现(顶点 $x$ 在相继边之间). 当然，在 $\mathcal{M}_x$ 中 $a$，$b$ 由两条边连结，如果它们相继出现两次，这不常发生. 显然，$\mathcal{M}_x$ 是 2 正则的. 顶点条件要求对每个顶点 $x$，$\mathcal{M}_x$ 是连通的(即一个单一的多边形).

在一个连通图里，由网出发这种粘贴构造的拓扑空间是一个曲面，当且仅当网满足顶点条件. 图 $G$ 在这个曲面上有自然的嵌入. 例 35.3 中的网满足顶点条件. 见例 35.4 和图 35.6.

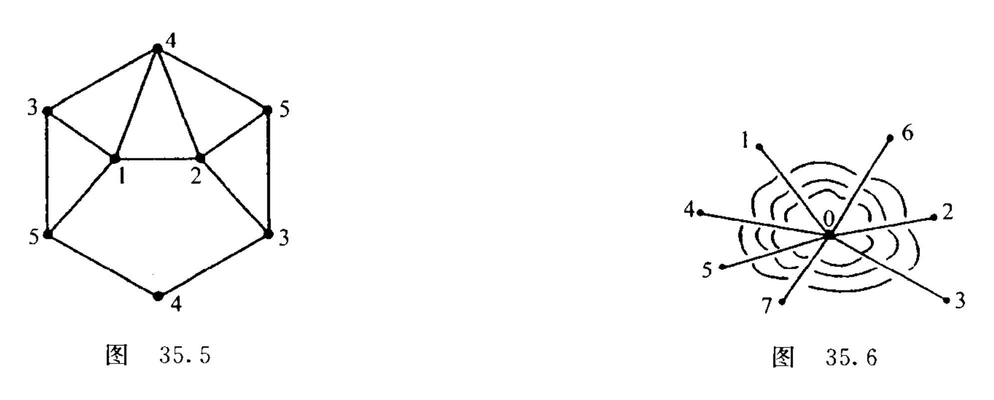



图 35.5 图 35.6

为了发现从一个网 $\mathcal{M}$ 构造了何种曲面 $\mathcal{S}$，首先计算欧拉特征 $h := |\mathcal{M}| - |E(G)| + |V(G)|$. 根据定理 35.1，如果 $h$ 是奇数，一定有 $\mathcal{S} = \mathcal{N}_{2-h}$. 但是如果 $h$ 为偶数，必须确定该曲面是否可定向(除了 $h=2$，此时球是唯一的可能)：如果 $\mathcal{S}$ 是可定向的，$\mathcal{S} = \mathcal{T}_{1-h/2}$；否则 $\mathcal{S} = \mathcal{N}_{2-h}$. 我们不加证明地陈述 $\mathcal{S}$ 是可定向的，当且仅当存在步路的定向(对每一条步路，选择两种可能方向中的一个)使得在每一个方向上，每条边恰被经过一次，在这种情形我们说网是可定向的.

容易检查符合顶点条件的网是否是可定向的. 我们给一条步路一个方向，定出与这个路径共享一条边的所有路径的方向，依次定出更多路径的方向. 顶点条件蕴涵在一个网中每条路径的方向是确定的. (为什么?)然后我们检查每一条边，看看经过它时沿什么方向.

495～497

**例 35.3(续)** 网 $\mathcal{M}_1$ 提供了 $K_5$ 在实射影平面 $\mathcal{N}_1$ 上的一个嵌入. 网 $\mathcal{M}_2$ 是可定向的——步路可以在它们被写下时定向，我们有 $K_5$ 在双环面 $\mathcal{T}_2$ 上的一个 2-胞腔嵌入.

在此后的例子中描述简单图中的步路时，我们在方括号里列出顶点序列，但略去终止的顶点，因为它与开始的顶点相同. 称长度为 3，4，…的路径为三角形，四边形，等等，忽略图中步路和多边形子图之间的差异是方便的.

**例 35.4** 我们证明 $K_8$ 能嵌入在双环面 $\mathcal{T}_2$ 上. 这表明对 $\mathcal{T}_2$ 的染色至少需要 8 种颜色，并证明 $g=2$ 时的 Heawood 猜想.

一定有 18 个面(所以 $f-e+v=-2$)，且它们的度加起来一定是 56. 下面展示有 2 个四边形和 16 个三角形作为面的一个解. 我们用“差方法”(参见第 19 章).

我们取$\mathbb{Z}_8$，整数模 8 作为 $K_8$ 的顶点. 两个四边形的顶点序列为[0，2，4，6]和[1，3，5，7].

三角形是两个初始三角形[0，1，4]和[0，3，2]的模 8 平移．读者应检查每条边恰出现在两条步路中．我们来检查顶点条件．因为模 8 平移保持多边形，所以只需检查顶点 0．经过 0 的路径为[0，2，4，6]，[0，1，4]，[7，0，3]，[4，5，0]，[0，3，2]，[5，0，7]和[6，1，0]．它们结合在一起构成图 35.6 中所示的单独一个多边形．

剩下要检查这个网是否是可定向的．网可定向，如果两个四边形定向为[0，2，4，6]和[7，5，3，1]，且每隔一个三角形被反向(当初始三角形被$\mathbb{Z}_8$的一个奇元素平移时)，由此得到一个可定向的网．

**问题 35A** 找出 $K_5$ 中 5 个四边形的网、$K_6$ 中 6 个五边形的网和 $K_7$ 中 7 个六边形的网，它们都满足顶点条件．你构造了什么曲面？

**问题 35B** 在克莱布什(Clebsch)图中找出 16 个五边形的网(见例 21.4)．既检查顶点条件又检查可定向性．如果有任何曲面被构造出来，它是什么曲面？相对于这个嵌入的对偶图是什么？

**问题 35C** (i)证明：如果一个简单图 $G$ 被嵌入在不可定向的曲面$\mathcal{N}_g(g\geqslant 1)$上，则 498

$$\chi(G)\leqslant\frac{7+\sqrt{1+24g}}{2}.$$

(ii)证明：如果一个简单图 $G$ 被嵌入到克莱因瓶$\mathcal{N}_2$ 上，则或者它有度$\leqslant 5$ 的一个顶点，或者是 6 正则的．证明在 $K_7$ 中有 14 个三角形的一个唯一的网，它满足顶点条件且是可定向的，因此 $K_7$ 不能嵌入到克莱因瓶上．对嵌入到$\mathcal{N}_2$ 上的图 $G$ 得出$\chi(G)\leqslant 6$ 的结论．

(毕竟 $K_7$ 不能嵌入到克莱因瓶上．我们得出结论：对嵌入到$\mathcal{N}_2$ 上的图 $G$，$\chi(G)\leqslant 6$．)

**问题 35D** 在继续讨论除球之外的曲面之前，我们说对网的理解使我们对如下事实有一个简洁的证明：如果 $G$ 和 $H$ 是不可分的惠特尼对偶，则相对于同构于 $H$ 的对偶 $G^*$，在球上存在 $G$ 的一个嵌入．如在定理 34.2 的证明中，与 $H$ 的一个顶点关联的边的集合在 $G$ 中是一个回路．在 $G$ 中得到的步路系是一个网$\mathcal{M}$．证明$\mathcal{M}$满足顶点条件．解释所构造的曲面为何是球以及 $G^*$ 的对偶为何同构于 $H$．

**问题 35E** 考虑一个连通图 $G$ 和 $G$ 中满足顶点条件(即地图)的网$\mathcal{M}$．为了简化问题，假设 $G$ 是简单的且在$\mathcal{M}$中的步路是简单闭路——我们把它们等同于多边形并称之为面．这张地图的一个自同构是 $V(G)$的一个置换，它把边变为边，面变为面(即 $G$ 的一个自同构保持$\mathcal{M}$)．证明：如果一个自同构 $\alpha$ 保持一个顶点 $x$、与 $x$ 关联的一条边 $e$ 以及与 $e$ 关联的一个面 $F$ 不动，则它是恒等的．

(由此，如上面所说，图 $G$ 的一个简单地图至多有 $4\mid E(G)\mid$ 个自同构．等号成立的例子包括柏拉图立体以及例 35.1 和例 35.2 中的地图．)

**定理 35.4** *如果 $n\equiv 7(\mathrm{mod}\ 12)$，则完全图 $K_n$ 在亏格为* 499

$$g:=(n-3)(n-4)/12$$

*的可定向曲面上有一个三角嵌入．*

**证明** 在 $K_n$ 中我们构造一个满足顶点条件的可定向的三角网．设 $n=12s+7$．我们用$\mathbb{Z}_n$作为 $K_n$ 的顶点．

构造在图 35.7 的图示中被编码. 图示的情形是 $n=7$，$n=19$，$n=31$ 和 $n=12s+7$.（在一般情形，竖直边交错定向且相继标号为 1，2，…，$2s$.）我们本可以不给图，而把这一构造作为差方法的一个应用简单地加以描述，但这样做不好，因为图示对寻找这一嵌入及其他嵌入时很有帮助.

注意边被从 1 到 $6s+3$ 的整数标号."守恒"定律或"基尔霍夫(Kirchhoff)电流定律"成立：在每个顶点，入边上的值之和等于出边上的值之和.（除没有发点或收点的情形外，这是第 7 章定义的强度为 0 的流.）

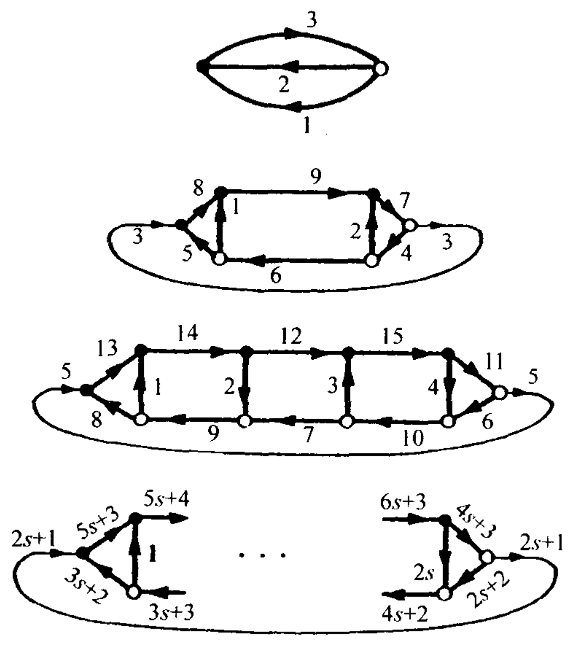



图 35.7

其实，认为所示的有向边的反转也出现是有帮助的；在图 35.7 中边的反转的标号将等于已出现的边的标号的相反数. 那么模 $n=12s+7$ 的所有非零值出现在有向边上，每个值恰好一次. 顶点有两种类型：实心的（代表"顺时针方向"）和空心的（代表"逆时针方向"）.

在图 35.7 的图示中，每个顶点提供 $K_n$ 中 $n$ 个有向三角形的一个族，它们模 $n$ 彼此是平移. 对每个实心顶点，是按照顺时针顺序值为 $a$，$b$，$c$ 的三条有向边的尾，取 $n$ 个有向三角形

$$[x,x+a,x+a+b],\quad x\in\mathbb{Z}_n.$$

回忆在$\mathbb{Z}_n$中 $a+b+c=0$，如果取$[y,\ y+b,\ y+b+c]$($y\in\mathbb{Z}_n$)或$[z,\ z+c,\ z+c+a]$($z\in\mathbb{Z}_n$)，则得到相同的三角形. 对每个空心顶点，它是按照逆时针顺序值为 $a$，$b$，$c$ 的三条有向边的尾，取 $n$ 个有向三角形

$$[x,x+a,x+a+b],\quad x\in\mathbb{Z}_n.$$

例如，在图 35.7 的第三个图示中($n=31$)，有一个空心顶点的入边标号为 7 和 2，一条出边标号为 9. 我们把它看作是标号为 $-7$，$-2$ 和 9（逆时针方向）的出边，取$[0,\ -7,\ -9]$的平移（或$[0,\ 9,\ 2]$或$[0,\ -2,\ 7]$的平移）模 31 得到的 31 个有向三角形. 在这个图示中另一个顶点由$[0,\ 14,\ 13]$模 31 的平移产生 31 个有向三角形.

500 ~ 501

不难看出，从图示中得到的有向三角形的集合构成一个定向的三角网. 例如，当 $n=31$ 时，为了找到一个三角形沿 4 到 23 的方向经过连结 4 到 23 的边，注意到在$\mathbb{Z}_n$中 $23-4=-12$. 标号为 $-12$ 的边与标号为 15 和 $-3$ 的出边离开一个实心顶点，找到三角形$[4,\ 4+(-12),\ 4+(-12)+15]=[4,\ 23,\ 7]$. 按 23 到 4 的方向经过连结 23 到 4 的边的三角形是$[23,\ 4,\ 6]$.

对 0 检验顶点条件就够了. 设 $e_i$ 表示 $K_n$ 中的边$\{0,\ i\}$. 考虑网中经过 0 且边 $e_a$ 进入 0 的三角形. 在图示中，标号为 $a$ 的边进入一个顶点，比如说，这个顶点是按顺时针或逆时针顺序标号为$-a$，$p$，$q$ 的边的尾，顺序取决于顶点是实心的还是空心的. 也就是说，三角形是$[a,\ 0,\ p]$且在边 $e_p$ 上离开 0. 总之，如果一个三角形在 $K_n$ 的边 $e_i$ 上进入 0，从图示中找到 $j$ 的值使

该三角形在 $e_j$ 上离开 0 如下：在图示中找到标号为 $i$ 的边——适当地按顺时针方向或逆时针方向在这条边进入的点转动并在下一条边离开——在图示中离开的边上的标号是 $j$.

例如，当 $n=31$ 时，我们得到 $K_n$ 的边 $e_{i_\ell}$ 的序列，使得在 $e_{i_\ell}$ 进入 0 的三角形在 $e_{i_{\ell+1}}$ 离开，该序列是

$$e_1, e_{-13}, e_{-8}, e_{-9}, e_{-7}, e_{-10}, e_{-6}, e_5,$$
$$e_{13}, e_{14}, e_{12}, e_{15}, e_{11}, e_6, e_{-4}, e_{-15}, e_{-3}, e_7, e_{-2}, e_{-14},$$
$$e_{-1}, e_8, e_{-5}, e_{-11}, e_4, e_{10}, e_3, e_{-12}, e_2, e_9, e_1, \cdots$$

上面相继的对在 $\mathcal{M}_0$ 中相邻，这是一个单一的多边形. 读者应检验在图 35.7 的每个图示中，这个方法类似地产生沿每个方向经过图示的每条边一次的一个序列. 这是非常令人惊奇的. ■

**问题 35F** (i)如果完全图 $K_n$ 在可定向的曲面 $\mathcal{T}_g$ 上有一个嵌入使得所有的面以三角形为界，则 $g=(n-3)(n-4)/12$.

(ii)如果完全二部图 $K_{n,n}$ 在可定向的曲面 $\mathcal{T}_g$ 上有一个嵌入使得所有的面以四边形为界，用 $n$ 表示 $g$ 的表示式是什么？当 $n>2$ 时，存在这样一个嵌入的 $n$ 的最小值是什么？

为了尽快且尽可能简单地给出定理 35.8 的证明，我们采用了与原来的上下文不相宜的一个构造. 本章以对一些想法的简要讨论结束，这些想法使 Ringel 和 Youngs 提出了对 $n$ 的所有值的嵌入方法.

502

J. Edmonds(1960)描述了图在可定向曲面上嵌入的一个技巧. 可以认为这个技巧源自相对该嵌入的对偶图中的网. 如果我们有简单连通图 $G$ 在可定向曲面 $\mathcal{S}$ 上的一个嵌入，则在 $\mathcal{S}$ 上一个定向的选择将在每个顶点引起与这个点关联的边的一个循环排列. Edmonds 指出，任意一个这样的"局部循环排列"确定一个嵌入. 设 $G$ 是一个简单图. 假设对每个点 $x$，给定与 $x$ 关联的边的集合 $S(x)$ 的一个排列 $\sigma_x$. 然后确定一个自然的定向网 $\mathcal{M}$ 如下. 如果有向路径经过一条边 $e$，$e$ 的定向是从其端点 $y$ 到 $x$，跟着 $e$ 的边是 $\sigma_x(e)$.

下面的例子涉及简单图，因此局部排列可以缩短为相邻顶点的排列且步路可以用它们的顶点序列描述.

**例 35.5** 考虑 $K_5$，其顶点集为{1，2，3，4，5}且有如下的局部排列：

$$1:(2435)$$
$$2:(1435)$$
$$3:(4125)$$
$$4:(1325)$$
$$5:(1234).$$

把得到的路径作为 5 个顶点的完全有向图的边的分解考虑可能是有益的. 设 $e_{ij}$ 表示方向从 $i$ 到 $j$ 的边. 这里是路径的边：

$$(e_{12}, e_{24}, e_{45}, e_{51}),$$
$$(e_{13}, e_{32}, e_{25}, e_{53}, e_{34}, e_{42}, e_{23}, e_{35}, e_{54}, e_{41}),$$
$$(e_{14}, e_{43}, e_{31}, e_{15}, e_{52}, e_{21}).$$

这些路径的顶点序列正好是例 35.3 中 $\mathcal{M}_2$ 的顶点序列.

对图 35.7 中有 $4s+2$ 个顶点的图的族，我们通过用实心顶点指示局部排列是顺时针方向

503

的和空心顶点指示局部排列是逆时针方向的来指定每个顶点的循环顺序. 作为定理 35.8 的证明的一部分，我们必须检查作为结果的嵌入恰有一个面.

给定一个有限群 $\Gamma$ 和 $\Gamma$ 的非单位元元素的一个子集 $S$ 使得 $\alpha\in S$ 蕴涵 $\alpha^{-1}\in S$，凯莱图 $G(\Gamma, S)$ 是顶点集为 $\Gamma$ 且顶点 $\alpha$ 和 $\beta$ 相邻当且仅当 $\beta\alpha^{-1}\in S$ 的简单图. 完全图 $K_n$ 是相对于任何一个 $n$ 阶群的凯莱图，这里 $S$ 由所有的非单位元构成. 通常要求 $S$ 生成 $\Gamma$——这保证对应的凯莱图是连通的.

W. Gustin(1963)引入“商流形”理论并发展了把凯莱图嵌入到可定向曲面的方法. 限于篇幅，这里不精确地描述这一理论，只给出几个例子. 考虑在凯莱图中，在顶点的局部排列是与 0 相邻的顶点的集合 $S$ 的一个初始循环排列$(s_1 s_2 \cdots s_k)$的所有“迁移”；也就是说，在 $\alpha$ 的局部排列是

$$(s_1+\alpha \quad s_2+\alpha \quad \cdots \quad s_k+\alpha)$$

(用加法符号).

**例 35.6** 考虑 $K_7$，其顶点集为{0, 1, 2, 3, 4, 5, 6}且在 $i$ 的局部排列$(1+i \quad 3+i \quad 2+i \quad 6+i \quad 4+i \quad 5+i) \pmod 7$如下：

0：(132645)
1：(243056)
2：(354160)
3：(465201)
4：(506312)
5：(610423)
6：(021534).

步路为

[1,2,4] [2,3,5] [3,4,6] [4,5,0] [5,6,1] [6,0,2] [0,1,3]
[3,5,6] [4,6,0] [5,0,1] [6,1,2] [0,2,3] [1,3,4] [2,4,5].

504

这是我们已经在例 35.2 看到的 $K_7$ 在环面上的三角嵌入.

例如，对以$\mathbb{Z}_{31}$为顶点集且初始局部排列为

$$(1,-13,-8,-9,-7,-10,-6,5,13,14,12,15,11,6,-4,$$
$$-15,-3,7,-2,-14,-1,8,-5,-11,4,10,3,-12,2,9)$$

的 $K_{31}$ 尝试这一方法，得到的三角网与定理 35.8 的证明中的相同. 图 35.7 中的图示实际上代表 $K_7$ 相对于前述嵌入的 $K_n$ 的对偶图的“商流形”. 对 $n=12s+7$，由图示表示的它嵌入的图有 $4s+2$ 个顶点、$6s+3$ 条边和 1 个面；由此得到的 $K_n$ 的嵌入有$(4s+2)n$ 个面、$(6s+3)n$ 条边和$(1)n$ 个顶点.

**问题 35G** 在$\mathbb{F}_q$中设 $\omega$ 是一个非零元素，这里 $q$ 是一个素数的幂. 比如说 $\omega$ 在$\mathbb{F}_q$的乘法群中的阶为 $m$，并设 $-1$ 是 $\omega$ 的一个幂. 考虑凯莱图 $G(\mathbb{F}_q, \langle\omega\rangle)$，这里$\langle\omega\rangle=\{1, \omega, \omega^2, \cdots\}$. 对凯莱图用加法群，因此 $a$ 和 $b$ 相邻当且仅当 $a-b\in\langle\omega\rangle$. (当 $\omega$ 是$\mathbb{F}_q$中的一个本原元时，凯莱图$(G(\mathbb{F}_q, \langle\omega\rangle)$是完全图；当 $q=16$ 和 $m=5$ 时，这个图是克莱布什图.)

我们取在 0 的局部排列为$(1, \omega, \omega^2, \cdots, \omega^{m-1})$，并作为迁移得到其他局部排列. 所得到

的网中的面的规模和数目是什么?

## 评注

P. J. Heawood(1861—1955)的大部分生涯是作为数学教授在英国的达累姆度过的，最后他担任副校长.

## 参考文献


G. Chartrand and L. Lesniak (1986), *Graphs and Digraphs*, 2nd edn., Wadsworth.

J. Edmonds (1960), A combinatorial representation for polyhedral surfaces, *Notices Amer. Math. Soc.* **7**, 646.

M. Fréchet and K. Fan (1967), *Initiation to Combinatorial Topology*, Prindle, Weber and Schmidt. 505

W. Gustin (1963), Orientable embedding of Cayley graphs, *Bull. Amer. Math. Soc.* **69**, 272–275.

G. Ringel (1974), *Map Color Theorem*, Springer-Verlag.

G. Ringel and J. W. T. Youngs (1968), Solution of the Heawood map coloring problem, *Proc. Nat. Acad. Sci. U.S.A.* **60**, 438–445.

A. T. White (1973), *Graphs, Groups, and Surfaces*, Mathematical Studies **8**, North-Holland. 506

# 第36章 电网络与方化正方形

我们以矩阵-树定理开始，它把一个图中生成树的数目表示为一个适当矩阵的行列式.

**定理 36.1** 在 $n$ 个顶点上无环的一个连通图 $G$ 中，生成树的数目是矩阵 $D-A$ 的任何一个 $(n-1)\times(n-1)$ 主子矩阵的行列式，这里 $A$ 是 $G$ 的邻接矩阵，$D$ 是一个对角矩阵，该矩阵的对角线上包含对应 $G$ 的顶点的度.

对没有环的多图 $G$，我们同意其邻接矩阵 $A$ 定义为，对不同的顶点 $x$ 和 $y$，$A(x, y)$ 等于连结 $x$ 和 $y$ 的边的数目. 我们发展一些工具之后再来证明这个定理，但现在给出几个例子.

**例 36.1** 设 $G$ 为图 36.1 中的图，则

$$D-A=\begin{bmatrix} 2 & -1 & 0 & -1 \\ -1 & 3 & -1 & -1 \\ 0 & -1 & 2 & -1 \\ -1 & -1 & -1 & 3 \end{bmatrix},$$

507

且 $G$ 有 8 棵生成树.

**例 36.2** 在定理 36.1 中，取 $G$ 为完全图 $K_n$. 在这种情形，矩阵 $D-A$ 是 $nI-J$，其中 $I$ 是 $n$ 阶单位阵，$J$ 是 $n\times n$ 的全幺矩阵. 可用几种方法(行运算、考虑特征值)计算这个简单矩阵的一个 $(n-1)\times(n-1)$ 主子矩阵的行列式，这留给读者作为练习. 这个习题完成之后，我们得到凯莱定理的另一个证明，参见第 2 章，完全图 $K_n$ 有 $n^{n-2}$ 棵生成树.

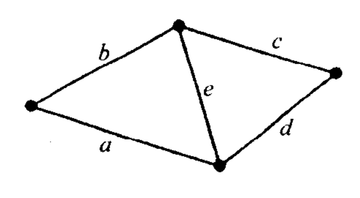



图 36.1

**问题 36A** 设 $M$ 为其线-和皆为 0 的 $n\times n$ 矩阵. 则 $M$ 的一个特征值是 $\lambda_1=0$，设 $\lambda_2$，$\lambda_3$，…，$\lambda_n$ 表示其他的特征值. 证明所有的 $(n-1)\times(n-1)$ 主子矩阵有相同的行列式，且这个值等于 $\frac{1}{n}\lambda_2\lambda_3\cdots\lambda_n$.

**例 36.3** 由上一问题的观察，计算已知谱的正则图的生成树的数目. 例如，设 $A$ 为彼得森图的邻接矩阵. 则 $A$ 有特征值

$$3,1,1,1,1,1,-2,-2,-2,-2$$

(见第 21 章). 矩阵 $M$ 是 $3I-A$，它有特征值

$$0,2,2,2,2,2,5,5,5,5.$$

我们得出彼得森图有 2000 棵生成树的结论.

下面的引理以柯西-比内(Cauchy-Binet)定理著称，更常见的叙述和应用是把下面的对角阵 $\Delta$ 取作单位阵.

**引理 36.2** 设 $A$ 和 $B$ 分别是 $r\times m$ 和 $m\times r$ 矩阵. 设 $\Delta$ 是第 $i$ 行第 $i$ 列的项为 $e_i$ 的 $m\times m$ 对角矩阵. 对 $\{1, 2, \cdots, m\}$ 的一个 $r$-子集 $S$，设 $A_S$ 和 $B^S$ 分别表示 $A$ 和 $B$ 的 $r\times r$ 子矩阵，它们是由 $A$ 的列或 $B$ 的行构成的，而这些行和列是由 $S$ 中元素指示的. 则

$$\det(A\Delta B)=\sum_S \det(A_S)\det(B^S)\prod_{i\in S}e_i,$$ 508

这里和取遍{1, 2, …, $m$}的所有 $r$-子集.

**证明** 我们在 $e_1$, …, $e_m$ 是独立的不定元的假定下证明这个引理. 当然，它对 $e_1$, …, $e_m$ 的所有值成立.

$r\times r$ 矩阵 $A\Delta B$ 的项是不定元 $e_1$, …, $e_m$ 的线性型；明确地，如果 $A=(a_{ij})$ 且 $B=(b_{ij})$，则 $A\Delta B$ 的($i$, $k$)项是 $\sum_{j=1}^{m}a_{ij}b_{jk}e_j$. 因此 $\det(A\Delta B)$是 $e_1$, …, $e_m$ 的次为 $r$ 的齐次多项式.

考虑一个单项式 $e_1^{t_1}e_2^{t_2}\cdots$，这里出现的不同的不定元 $e_i$(指数 $t_i>0$)的个数小于 $r$. 对不在 $e_1^{t_1}e_1^{t_2}\cdots$中出现的不定元用 0 代替，单项式 $e_1^{t_1}e_2^{t_2}\cdots$及其系数不受这一代替的影响. 但经过这一代替之后，$\Delta$ 的秩小于 $r$，因此多项式 $\det(A\Delta B)$的值是零多项式.

于是我们看到多项式 $\det(A\Delta B)$的一个单项式的系数是 0，除非该单项式是 $r$ 个不同的不定元 $e_i$ 之积，即它具有形式 $\prod_{i\in S}e_i$，这里 $e_i$ 是 $S$ 的某一 $r$- 子集. 在 $\det(A\Delta B)$ 中，单项式 $\prod_{i\in S}e_i$ 的系数可以通过设 $e_i$ 的值得到：$e_i$ 等于 1，$i\in S$；$e_j$ 等于 0，$j\notin S$. 当在 $\Delta$ 中作这一代替时，$A\Delta B$ 的值为 $A_SB^S$. 因此，在 $\det(A\Delta B)$中 $\prod_{i\in S}e_i$ 的系数是 $\det(A_S)\det(B^S)$. ■

本章着重讨论有向图. 所有的图论术语(树、分支、回路等)用于有向图，通过忽略边的方向得到基础无向图时意义不变. 因此，有向图中的一条路径会以“向前的”方向经过一条边，以“向后的”方向经过另一条边，我们真正感兴趣的是无向图，但为了研究理论，选择一个定向并产生一个有向图是方便的，任何一个定向都可以且产生本质上相同的理论.

如前面几章所做的，用泛函记号 $M(i, j)$表示矩阵 $M$ 第 $i$ 行第 $j$ 列的项，用 $f(i)$表示向量 $f$ 的第 $i$ 个坐标.

一个有向图 $H$ 的关联矩阵 $N$ 是其行由 $V(H)$指示、其列由 $E(H)$指示的矩阵，且这里 509

$$N(x,e)=\begin{cases}0 & \text{如果 } x \text{ 不与 } e \text{ 关联，或者 } e \text{ 是一个环，}\\ 1 & \text{如果 } x \text{ 是 } e \text{ 的首，}\\ -1 & \text{如果 } x \text{ 是 } e \text{ 的尾.}\end{cases}$$

我们提及

$$\operatorname{rank}(N)=|V(H)|-|C(H)|, \tag{36.1}$$

这里 $C(H)$是 $H$ 的分支的集合. 为了明白这一点，假定 $g$ 是一个行向量，其坐标由 $V(H)$指示且 $gN=0$. 这意味着对一个比如说从 $x$ 指向 $y$ 的边 $e$，$g(y)-g(x)=0$. 显然 $gN=0$ 当且仅当 $g$ 在 $H$ 的每个分支的顶点集上是常数，因此所有使得 $gN=0$ 的 $g$ 的空间的维数是 $|C(H)|$.

我们还提及，一个方阵的每一列至多有一个 1 且至多有一个 $-1$，所有其他项为 0，该方阵的行列式等于 0 或 $\pm1$. 这由归纳法得出：如果每列有一个 $+1$ 和一个 $-1$，则所有行的和是零向量，因此矩阵是奇异的. 否则，由仅有一个非零项的一列展开行列式，它等于 $\pm1$ 乘以一个有相同性质的较小的矩阵的行列式. 所以，一个有向图的关联矩阵的子方阵的行列式等于 0 或 $\pm1$.（有这一性质的矩阵称为全幺模的.）

**定理 36.1 的证明** 设 $H$ 为有 $n$ 个顶点的连通有向图，其关联矩阵为 $N$. 设 $S$ 为 $n-1$ 个

边的集合，用柯西-比内定理的记号，考虑关联矩阵 $N$ 的 $n\times(n-1)$ 子矩阵 $N_S$，它的列由 $S$ 的元素指示. 由(36.1)，$N_S$ 的秩为 $n-1$ 当且仅当 $H$ 以 $S$ 为边集的生成子图是连通的，即当且仅当 $S$ 是 $H$ 中一棵树的边集. 设 $N'$ 是从关联矩阵 $N$ 去掉任意一行得到的矩阵. 因为 $N$(或 $N_S$)的所有行的和是零向量，所以 $N'_S$ 的秩与 $N_S$ 的秩相同. 根据这一观察和上面的叙述证明

510

$$\det(N'_S)=\begin{cases}\pm 1 & \text{如果 } S \text{ 是 } H \text{ 中一棵生成树的边集,}\\ 0 & \text{否则.}\end{cases} \tag{36.2}$$

设给定 $n$ 个顶点的连通无环图 $G$，设 $H$ 是 $G$ 的任何一个定向，并设 $N$ 是 $H$ 的关联矩阵. 则 $NN^{\top}=D-A$，因为

$$NN^{\top}(x,y)=\sum_{e\in E(G)}N(x,e)N(y,e)$$

$$=\begin{cases}\deg(x) & \text{如果 } x=y,\\ -t & \text{如果在 } G \text{ 中 } x \text{ 和 } y \text{ 由 } t \text{ 条边相连.}\end{cases}$$

$D-A$ 的一个 $(n-1)\times(n-1)$ 主子矩阵具有形式 $N'N'^{\top}$，这里 $N'$ 由 $N$ 去掉任意一行得到. 由柯西-比内定理，

$$\det(N'N'^{\top})=\sum_S\det(N'_S)\det(N'^{\top}_S)=\sum_S(\det(N'_S))^2,$$

这里和取遍边集的所有 $(n-1)$-子集 $S$. 由(36.2)，这是 $G$ 的生成树的数目. ■

**注记** 如果把 $E(G)$ 视为不定元的一个集合并应用引理 36.2 于 $N\Delta N^{\top}$ 的 $(n-1)\times(n-1)$ 主子矩阵，这里 $\Delta$ 是对角矩阵，其行和列由边指示且对角线上的项是边自身(即 $\Delta(e,e):=e$)，可以发现 $\det(N\Delta N^{\top})$ 是对应于 $G$ 中树的边集的单项式的和. 例如，对图 36.1 中的图 $G$，

$$N\Delta N^{\top}=\begin{bmatrix}a+b & -b & 0 & -a\\ -b & b+c+e & -c & -e\\ 0 & -c & c+d & -d\\ -a & -e & -d & a+d+e\end{bmatrix}.$$

当然，$N\Delta N^{\top}$ 是一个奇异矩阵(所有的线-和为 0)，但通过去掉行和列，例如去掉最后一行和最后一列得到的 $3\times 3$ 矩阵的行列式是

511

$$(a+b)(b+c+e)(c+d)-b^2(c+d)-c^2(a+b)$$
$$=abc+abd+acd+ace+ade+bcd+bce+bde,$$

它代表 $G$ 中的 8 棵生成树.

下面给出定理 36.1 的一个推广，它属于 W. T. Tutte(1948)，该推广的证明较我们对第一个定理给出的证明短!(推广的陈述有一种类型的归纳法在原定理中不可用.)当我们把定理 36.3 用于从一个无向图通过把它的每条边换成一对有向边(一个方向一个)得到的有向图时，重新得到定理 36.1 的陈述.

**定理 36.3** 设 $G$ 是顶点为 $x_1, x_2, \cdots, x_n$ 的一个有向图. 定义矩阵 $M$ 或 $M(G)$ 如下：$M=(m_{ij})$，这里 $m_{ii}$ 是离开 $x_i$ 的边的数目，不计环，对 $i\neq j$，$m_{ij}$ 是从 $x_i$ 到 $x_j$ 的边数的相反数，则 $G$ 的以 $x_\ell$ 作为根的有向生成树(或树形图)的数目 $A_\ell$ 或 $A_\ell(G)$ 是 $M$ 中位置 $(\ell,\ell)$ 的子

式，即由矩阵 $M$ 去掉第 $\ell$ 行和第 $\ell$ 列得到的 $(n-1)\times(n-1)$ 主子矩阵的行列式.

**证明** 为了记号上的方便，我们取 $\ell=1$. 对某个 $i>1$，如果没有边离开 $x_i$，则定理的陈述成立：$M(G)$ 的行 $i$ 是零向量，位置(1，1)的子式和有向树的数目都是零.

对某个 $i>1$，如果有多于一条边离开 $x_i$，设 $G_1$ 和 $G_2$ 是有向图，除 $G$ 中离开 $x_i$ 的一些边($\geqslant 1$)被放在 $G_1$ 中且其余的边($\geqslant 1$)被放在 $G_2$ 中外，它们与 $G$ 相同，因为 $G$ 的每棵以 $x_1$ 为根的有向生成树必定恰好包含离开 $x_i$ 的一条边，所以 $A_1(G)=A_1(G_1)+A_1(G_2)$. 注意 $M(G)$，$M(G_1)$ 和 $M(G_2)$ 除第 $i$ 行外都是相同的，且 $M(G)$ 的第 $i$ 行等于 $M(G_1)$ 和 $M(G_2)$ 的第 $i$ 行之和. 因此，第一个矩阵中位置(1，1)的子式等于后两个矩阵中那些子式的和.

于是，对所有的 $i>1$ 使得 $m_{ii}=1$ 的有向图 $G$，验证定理的陈述就够了. 也就是说，要验证的图对 $i>1$，在任意顶点 $x_i$ 恰有一边离开.

如果在这样的有向图 $G$ 中有一条不经过 $x_1$ 的有向闭路，比如说 $x_2\to x_3$，$x_3\to x_4$，…，$x_k\to x_2$，则从行 2 到行 $k$ 的和为 **0** 且因此位置(1，1)的子式是 0. 从这些点中的任何一个开始，没有有向路到 $x_1$，因此没有有向生成树. [512]

如果在这样的有向图 $G$ 中没有有向闭路不经过 $x_1$，以任意一个顶点 $x_j$ 开始的有向路，随着遇到的每一个顶点的离开的边前进，一定到达 $x_1$. 我们看到这个有向图 $G$，当离开 $x_1$ 的边被删去(这些边不会出现在任何一棵有向生成树中)时，剩下的图本身是一棵有向生成树，所以 $A_1(G)=1$. 在 $M(G)$ 中，也可以知道位置(1，1)的子式是 1，例如用归纳法：由对应顶点 $x_j$ 的一个列 $j$ 展开行列式，在这一有向生成树中 $x_j$ 的入度为 0(因此在位置$(j，j)$上是 1 且在位置$(i，j)$ $(i>1，i\neq j)$上为 0). ■

我们说，如果一个有向图 $G$ 的边被看作独立的不定元且构成如 $M(G)$ 那样的矩阵，但这里项不是整数而是边的形式和，则子式是所有有向树的形式和，每棵树由其边的乘积表示. 读者容易修改上面的证明. 例如，如果 $G$ 是一个有向图，其顶点为 1，2，3，边 $a$ 从 2 指向 1，边 $b$ 从 3 指向 1，边 $c$ 从 3 指向 2，则考虑矩阵

$$M=\begin{bmatrix}0 & 0 & 0\\ -a & a & 0\\ -b & -c & b+c\end{bmatrix}.$$

位置(1，1)的子式是 $ab+ac$，它们代表以 1 为根的两棵有向树.

**问题 36B**(容易) 设 $T_n$ 为顶点 1，2，…，$n$ 上的边从 $j$ 指向 $i$(只要 $i<j$)的“可迁竞赛图”，$M(T_n)$ 是什么？在 $T_n$ 中以 1 为根的有向生成树的数目是什么？描述所有这样的有向树.

现在我们能给出关于德布鲁因序列数目的定理 8.2 的第二个证明. 设有向图 $G_n$ 如同第 8 章所定义的. $G_n$ 的所有入度和出度都等于 2. 在附录 1 中建议的问题 2B 的解法证明了 $G_n$ 中(有向)欧拉圈的数目等于 $G_n$ 中以任意一点为根的有向生成树的数目. 由定理 36.3 和问题 36A，这个数目可从对矩阵 $M(G_n)$ 的特征值的知识得出. [513]

由整数 0 到 $2^{n-1}-1$ 给规模为 $2^{n-1}$ 的矩阵 $B_n$ 的行和列编号. 如果 $j=2i$ 或 $2i+1 \pmod{2^{n-1}}$，设 $b_{ij}=1$. (注意 $B_n$ 的上半部分和下半部分是相同的.)则 $M(G_n)=2I-B_n$. 现在我们计算 $xI-M(G_n)$ 的行列式 $D_n(x)$. 对这个行列式下半部分进行明显的行运算和列运算，可以得到

$$D_n(x) = (x-2)^{2^{n-2}} D_{n-1}(x).$$

因为 $D_2(x)=x(x-2)$，我们看到 $M_n$ 的所有非零特征值等于 2，因此由问题 36A，长度为 $2^n$ 的德布鲁因圈的数目是

$$\frac{1}{2^{n-1}} \cdot 2^{2^{n-1}-1} = 2^{2^{n-1}-n}.$$

* * *

设 $N$ 为一个有向图 $H$ 的关联矩阵. $N$ 的行空间称为 $H$ 的上边缘空间；$N^{\top}$ 的零空间，即使得 $fN^{\top}=0$ 的所有行向量 $f$ 的空间，称为 $H$ 的圈空间. 它们在电网络和代数拓扑理论中是很重要的. 由(36.1)，一个有向图 $H$ 的上边缘空间的维数是 $|V(H)|-|C(H)|$，且因此其圈空间的维数是 $|E(H)|-|V(H)|+|C(H)|$.

由定义，一个向量 $f$ 是圈当且仅当对每个顶点 $x$，出边上的值 $f(e)$ 的和等于入边上的值 $f(e)$ 的和. 从 $H$ 中任意一个简单闭路 $p$ 如下得到一个圈 $f$(所谓的*初等圈*)：在路上向前的边定义 $f(e)$ 为 $+1$，在向后的边上定义 $f(e)$ 为 $-1$，不在路上的所有边上定义 $f(e)$ 为 0，这是圈 $f$ 的一个例子. 一个向量是上边缘当且仅当它与所有的圈正交，特别地，一个上边缘在一条简单闭路向前的边上的值之和等于在该路向后的边上的值之和.

[514]

**问题 36C** 一个向量 $g$ 的坐标由一个有向图 $H$ 的边 $E(H)$ 指示，$g$ 是 $H$ 上的一个上边缘，当且仅当对每一条闭步路 $w$，$g$ 在其边上的值的带符号的和($g$ 在 $w$ 的向前的边上的值之和减去 $g$ 在 $w$ 的向后的边上的值之和)是零.

约定电网络组成如下：一个有向图 $H$，与每条边 $e$ 相联系的函数 $r$(它给出 $e$ 的“电阻” $r(e)\geqslant 0$)，以及与每条边 $e$ 相联系的函数 $s$(它给出 $e$ 的“外加电动势”或“电压电源”$s(e)$). 也就是说，每条边被认为是电阻或电池，或者既是电阻又是电池. 如果电池和电阻被连结，“电流” $f(e)$ 将经过每条边且可测量过每条边的“势差”或“电压”$g(e)$. 这里我们需要知道的所有知识就是向量 $f$ 和 $g$ 能从 $r$ 和 $s$ 由称为*基尔霍夫定律和欧姆定律*的规则确定. 基尔霍夫电流定律和电压定律分别断言，$f$ 是一个圈且 $g$ 是一个上边缘. 欧姆定律说 $g(e)=-s(e)+r(e)f(e)$，或者用矩阵的记号，$g=-s+fR$，这里 $R$ 是数 $r(e)$ 在对角线上的对角矩阵，这里把 $s$，$g$，$f$ 作为行向量.

**问题 36D** 假设 $\{e : r(e)=0\}$ 不包含回路，即这个集合是一个森林的边集. 证明电网络有唯一的一个解，这意味着有这样一个集合，对任意 $s$ 存在唯一的向量 $f$ 和 $g$ 满足以上定律.

*方化矩形*是指一个矩形被剖分成数目有限的正方形. 两个例子见图 36.2 和图 36.3. 这两个矩形的大小分别为 $33\times 32$ 和 $177\times 176$. 当方化矩形内的正方形有不同的规模且不包含较小的方化矩形时，它们被认为是优美的.

**问题 36E** 寻找在图 36.4 中较小的正方形的整数边长，使得该图表示一个方化矩形.

多年以来，人们不知道一个*正方形*是否能剖分成有限个不相等的较小的正方形. 在 20 世纪 30 年代后期，这样的方化正方形最终被发现. 一个例子展示在《Journal of Combinatorial Theory》的封面上，直到 A. J. W. Duijvestijn(1978)发现一个较小的例子；封面在 1979 年 1 月被更新. 这是可以剖分的最小可能的正方形(21). 计算机被用于得到这些结果，但研究方化矩形的一个重要工具是这一主题与电网络的联系，这个工具在 1936～1938 年被剑桥的四名大学生发现. 关于他们的工作的一个通俗的叙述由 W. T. Tutte(1961)和(1965)给出，Tutte 是发现者之一.

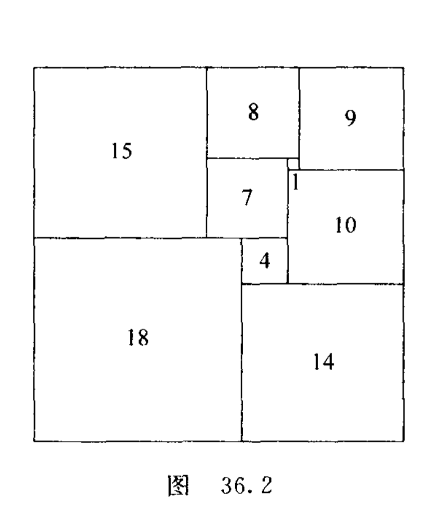


图 36.2

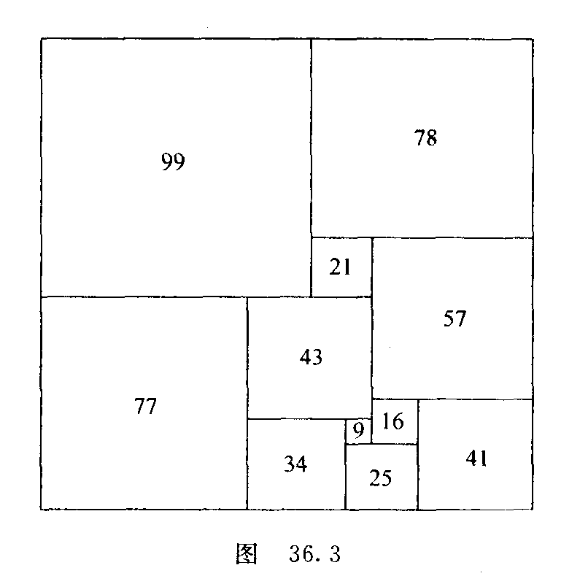


图 36.3

下面给出方化矩形和电网络联系的一个通俗描述. 对有一个显著边 $e_0$ 的电网络，使得对 $e\neq e_0$，$s(e)=0$，且这里

$$r(e)=\begin{cases}1 & \text{如果 } e\neq e_0,\\ 0 & \text{如果 } e=e_0.\end{cases}$$

我们用特殊网络一词. 也就是说，我们有由单位电阻和单个电池组成的一个系统.

起源于方化矩形的一个特殊电网络如下. 定义一个有向图 $H$，其顶点是图示中最大的水平线段. $H$ 的边是小正方形，并且对整个矩形包括一个特殊的边 $e_0$. 指定每条边($e_0$ 除外)方向向下，即指向较低的线段. 在图 36.5 中展示了一个例子. 显然有向图 $H$ 是平面的. 有一个实数 $f(e)$ 自然地与边 $e$ 相联系，即对应的小正方形的规模；取 $f(e_0)$ 是较大的矩形的宽度. 不难看出，$f$ 是 $H$ 上的一个圈：对每条最长的水平线段，"坐在"该线段上的正方形的边长之和等于"吊在"它之上的正方形的边长之和. 此外，如果不是有特殊的边，$f$ 就是一个上边缘：如果对每个顶点(水平线段)$x$，取 $h(x)$ 是从大矩形的上面的边起到 $x$ 对应的线段的距离，那么对 $e\neq e_0$，$f(e)$ 等于 $h(e$ 的首$)-h(e$ 的尾$)$. 因此，如果设 $s(e_0)$ 为矩形的高度并取 $g$ 为 $h$ 的上边缘，则 $f$ 和 $g$ 是电流向量和电压向量，它们解答了这个特殊的网络，即 $g=-s+Rf$.

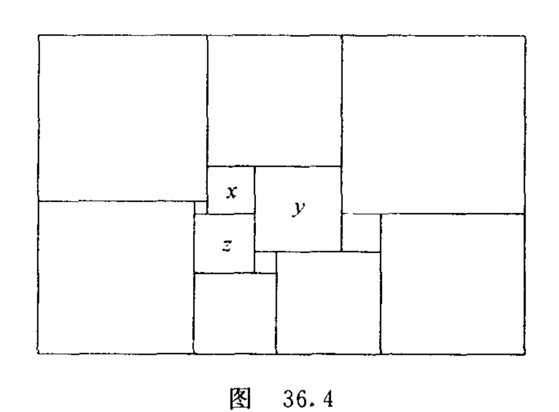
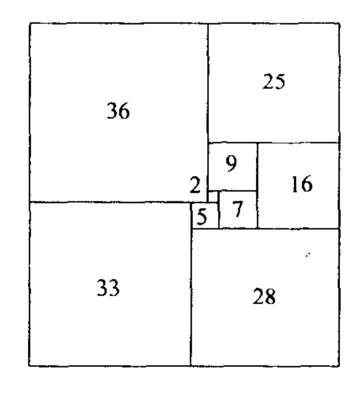


图 36.4



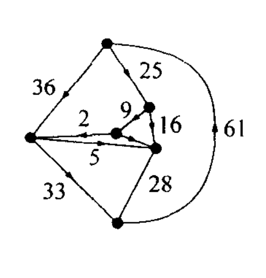
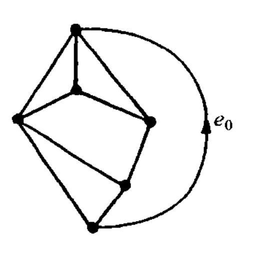



图 36.5

反之，一个特殊的电网络导致方化矩形的构造，这里有向图是平面的. 我们不给出证明. 矩形的宽度比高度等于网络的解中电流 $f(e_0)$ 比电压 $-g(e_0)$. (在网络的解中，有些边可能有负的电流，但我们可以反转这些边的方向以得到正值. 可删去或收缩电流为零的边，它们不会产生正方形.)因此一个方化正方形对应电阻器的一个平面网络，电阻器的净阻碍作用是 1 欧姆.

515 ~ 518

**问题 36F** 以你希望的任何方式解图 36.6 中的特殊网络，并画出对应的方化矩形. 对偶图也可被认为是特殊网络——从这些对偶网络中得到的方化矩形是什么?



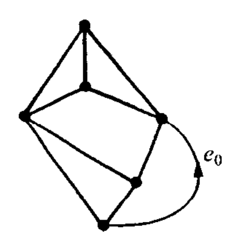




图 36.6

设 $N$ 是一个有向图 $D$ 的关联矩阵且 $\Delta$ 是由 $E(D)$ 指示的对角矩阵，$\Delta(e, e)=r(e)>0$，$r(e)$ 为边 $e$ 的电阻；设 $C := N\Delta^{-1}N^{\top}$. 如果一条附加边 $e_0$ 从 $D$ 的一个顶点 $y$ 指向另一个顶点 $x$，并且在这条边上施加一个充分的电源电压，使得电流 $f(e_0)$ 通过它，则基尔霍夫定律蕴涵穿过连结顶点 $a$ 到顶点 $b$ 的一条边 $e$ 的势差 $g(e)$，比如说，由

$$g(e) = \frac{f(e_0)}{\tau(D)}(xy.\,ab) \tag{36.3}$$

给出，这里 $(xy.\,ab)$ 表示 $C=(c_{ij})$ 的元素 $c_{xa}$ 的余子式中元素 $c_{yb}$ 的余子式，$\tau(D)$ 表示 $D$ 的生成树的数目($D$ 的复杂性). 见 Jeans(1908).

这个结论的一个结果是如下定理.

**定理 36.4** *如果在图 $G$ 的一个特殊网络的显著边 $e_0$ 上，电源电压 $s(e_0)$ 取作边 $e_0$ 上的生成树的数目，则得到的电流的所有值 $f(a)$ 为整数，且通过显著边 $e_0$ 的电流 $f(e_0)$ 等于不在边 $e_0$ 上的生成树的数目.*

**证明** 在定理陈述之前的讨论中，取 $D$ 为 $G'_{e_0}$ 的一个定向且 $\Delta$ 为单位矩阵. 如果电流 $f(e_0)$ 是 $\tau(D)=\tau(G'_{e_0})$，则由(36.3)，显然 $f(a)=g(a)$ 的所有值是整数. 剩下的只是证明 $-g(e_0)$ 等于边 $e_0$ 上的生成树的数目.

由(36.3)，$g(e_0)=(xy.\,yx)=-(xy.\,xy)$. 由定义，$(xy.\,xy)$ 是矩阵 $N''N''^{\top}$ 的行列式，这里 $N''$ 由 $N$ 删去行 $x$ 和行 $y$ 得到. 由柯西-比内定理，这等于

$$\sum_S (\det(N''_S))^2,$$

519

这里和取遍边集的所有 $(n-2)$-子集 $S$，且 $N''_S$ 是其行由 $S$ 的元素指示的 $N''$ 的子方阵.

通过观察 $\det(N''_S)$ 等于 0，除非 $S\cup\{e_0\}$ 是 $G$ 中一棵生成树的边集，在这种情况下 $\det(N''_S)$ 等于 $\pm1$ 而完成证明. 这与(36.2)的证明类似，留给读者作为练习. ■

总之，定理 36.4 说，$G$ 的一条边 $e_0$ 两端之间的电阻，当所有其他的边被视为单位电阻器时，是比值 $\tau(G''_{e_0})/\tau(G'_{e_0})$. 当 $G$ 是多边形或键图时，读者可以验证这与它们的电网络知识相符. 当我们找到一个平面图 $G$ 且有一边 $e_0$ 使得 $\tau(G''_{e_0})=\tau(G'_{e_0})$ 时，出现一个方化正方形. 仅这个陈述不一定对寻找方化正方形有帮助(无论如何，电机工程师会认为这是浪费电阻器). 这样

的图非常罕见.

## 评注

利用不等的正方形组成一个矩形的问题第一次出现的文献似乎是 M. Dehn(1903).

方化正方形的详表首先由 C. J. Bouwkamp, A. J. W. Duijvestijn, and P. Medema(1960)发表.

W. T. Tutte(1918—)[⊖]对图论作出了许多显著贡献. 他曾任滑铁卢大学组合与优化系名誉数学教授，该系是世界上少数几个系名中包括“组合”的学术系之一.

定理 36.3 的证明，参见 De Bruijn and Van Aardenne-Ehrenfest(1951).

前面提到的四名剑桥学生，其中的 C. A. B. Smith 对他们的合作经历写了一篇很好的文章，名字是“Did Erdös save Western Civilization?”(见 Graham and Nešetřil(1997).)很显然，埃德斯(Erdös)猜测一个正方形分解成较小的正方形一定包含相同大小的正方形. 这件事引起另一个人，即塔特(Tutte)在 Bletchley 庄园而不是在战场上终结该问题. 谣传他在那里为破译 Enigma 提供了关键线索，这解释了论文的标题.

## 参考文献


N. G. de Bruijn and T. van Aardenne-Ehrenfest (1951), Circuits and trees in oriented linear graphs, *Simon Stevin* **28**, 203–217. [520]

C. J. Bouwkamp, A. J. W. Duijvestijn, P. Medema (1960), *Tables relating to simple squared rectangles of order nine through fifteen*, T. H. Eindhoven.

A. J. W. Duijvestijn (1978), Simple perfect squared square of lowest order, *J. Combinatorial Theory* (B) **25**, 555–558.

M. Dehn (1903), Zerlegung von Rechtecke in Rechtecken, *Math. Ann.* **57**.

R. L. Graham and J. Nešetřil (Eds.) (1997), *The Mathematics of P. Erdős*, Springer.

J. H. Jeans (1908), *The Mathematical Theory of Electricity and Magnetism*, Cambridge University Press.

W. T. Tutte (1948), The dissection of equilateral triangles into equilateral triangles, *Proc. Cambr. Phil. Soc.* **44**, 463–482.

W. T. Tutte (1961), Squaring the square, in: M. Gardner, *The 2nd Scientific American Book of Mathematical Puzzles and Diversions*, Simon and Schuster.

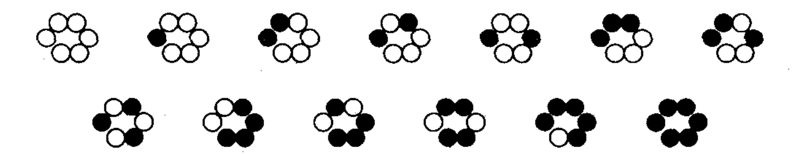
W. T. Tutte (1965), The quest of the perfect square, *Amer. Math. Monthly* **72**, No. 2, 29–35. [521]


⊖ Tutte 已于 2002 年去世. ——译者注

# 第 37 章　波利亚计数理论

本章返回到计数的讨论．有许多这样的例子，我们不关心原始对象的数目，而是关心相对于一个适当的等价关系来说等价类的数目．而且，这些等价关系经常以自然的方式由特定的置换群导出．

**问题 1**　两种颜色的 $n$ 个珠子能制成多少种"本质上不同"的项链？当 $n=6$ 时，由观察，这个数目是 13.



注意，我们认为项链

和　　(37.1)

本质上是相同的，因为通过垂直轴的反射(或翻转)可以从一个得到另一个．显然，在概念"本质上不同"的背后是正 $n$ 边形自同构的二面体群 $D_n$.

**问题 2**　$n$ 个顶点的不同构的简单图的数目是多少？对 $n=4$，有 11 个不同构的简单图．

**问题 3**　用 $n$ 种颜色给立方体的面(或者边，或者顶点)染色，本质上不同的方法数是多少？

522

**问题 4**　给定三个白球和一个黑球，把它们分配到两个方盒子和一个圆盒子中的方法数是多少？

| | | | |
|---|---|---|---|
| [○○○●][]() | [○○○][●]() | [○○][○●]() | [○○●][○]() |
| [○○○][](●) | [○○][○](●) | [○○●][](○) | [○○][●](○) |
| [○●][○](○) | [○●][](○○) | [○][●](○○) | [○○][](○●) |
| [○][○](○●) | [●][](○○○) | [○][](○○●) | [][](○○○●) |

设 $A$ 和 $B$ 是有限集，$G$ 是 $A$ 的一个置换群(或者更一般地，作用于 $A$ 上的一个有限群)．称 $B$ 的元素为*颜色*．群 $G$ 作用在映射 $f: A \to B$ 的集合 $B^A$ 上，当 $\sigma \in G$ 且 $f \in B^A$ 时，由

$$(\sigma(f))(x) := f(\sigma^{-1}(x))$$

定义 $\sigma(f) \in B^A$．在上面的前三个问题中，我们希望计数的是适当的群 $G$ 作用在集合 $B^A$ 上的轨道．

(在上式右边用 $\sigma^{-1}$ 而不用 $\sigma$ 不是一个错误．需要保证 $\sigma(\tau(f)) = (\sigma\tau)(f)$，这对 $G$ 在 $B^A$ 上有一个合法的"作用"是必需的．形式上，我们有 $G$ 同态于 $B^A$ 上的对称群．)

在项链问题中，我们把 $A$ 取作正 $n$ 边形的顶点集，$G$ 作为它的自同构群表示为顶点上的一个置换群(即 $2n$ 阶的二面体群 $D_n$ 的通常表示)．当所有的珠子不是圆的，而是一边是平的时，

问题稍有不同．那么，项链不能翻转，而且(37.1)中的那些项链被认为是不同的．

这里，取 $G$ 为 $n$ 阶循环群的正则表示；参见例 10.5.

在我们提出的问题中，最简单的是寻求映射的轨道数．进一步地，我们想知道给定“重量”的轨道数；例如，有 $n$ 个珠子的项链的数目，其中 $k$ 个是白色的，或者有 $n$ 个顶点和 $k$ 条边的图的数目．我们可引入 $B$ 上的一个置换群，并且关于一个更一般的等价关系寻找“构形”的数目．(这对分布问题是必需的．)

523

下面从回顾定理 10.5(伯恩赛德引理)开始：一个集合 $X$ 上的有限群 $G$ 的轨道数是不动点的平均数，即

$$\frac{1}{|G|}\sum_{\sigma\in G}\psi(\sigma), \tag{37.2}$$

这里 $\psi(\sigma)$ 表示在置换 $\sigma$ 下，$X$ 中的不动点数．从计算使得 $\sigma(x)=x$ 成立的有序对 $(x,\sigma)\in X\times G$ 的数目得出这个公式．

**定理 37.1** *设 $A$ 和 $B$ 是有限集且群 $G$ 作用在 $A$ 上．用 $c_k(G)$ 表示 $G$ 在 $A$ 上的圈分解中恰有 $k$ 个圈的置换数．则 $G$ 在所有映射 $f: A\to B$ 的集合 $B^A$ 上的轨道数是*

$$\frac{1}{|G|}\sum_{k=1}^{\infty}c_k(G)\,|B|^k.$$

**证明** 由伯恩赛德引理，由(37.2)给出轨道的数目，(37.2)中的 $\psi(\sigma)$ 在这里是使得 $\sigma(f)=f$，即对所有的 $a\in A$，$f(a)=f(\sigma^{-1}(a))$ 的映射 $f: A\to B$ 的数目．但映射 $f$ 被 $\sigma$ 固定，当且仅当 $f$ 在 $\sigma$ 的每个圈上是一个常数，读者应对此加以验证．这样的映射通过分配 $B$ 的一个元素到 $\sigma$ 的每个圈而得到，于是，如果 $\sigma$ 有 $k$ 个圈，被 $\sigma$ 固定的映射 $f$ 的数目是 $|B|^k$. ∎

读者最好在此停顿一下，验证当定理 37.1 用于上面的问题 1 时，将给出项链计数问题的答案：13.

因为后面将广泛使用这个定理，所以接下来介绍置换群的圈指标．首先，在本章中，用古老的记号 $(1^{k_1}2^{k_2}\cdots n^{k_n})$ 表示整数 $n$ 的分拆是方便的，它表示整数 $n$ 有 $k_i$ 个大小为 $i$ 的部分的分拆，其中 $i=1, 2, \cdots, n$. 这仅仅是一个记号，并不计算幂或乘积．

524

对集合 $A$ 的一个置换 $\sigma$，设 $z_i(\sigma)$ 表示 $\sigma$ 长度为 $i$ 的圈的数目；因此 $(1^{z_1(\sigma)}2^{z_2(\sigma)}\cdots)$ 是 $n=|A|$ 的一个分拆，称为 $\sigma$ 的类型．给定一个作用在 $A$ 上的群 $G$，我们把圈指标 $Z_G$ 定义为 $n$ 个字母 $X_1, X_2, \cdots, X_n$ 的一个多项式

$$Z_G(X_1,X_2,\cdots,X_n):=\frac{1}{|G|}\sum_{\sigma\in G}X_1^{z_1(\sigma)}\cdots X_n^{z_n(\sigma)}.$$

定理 37.1 断言 $B^A$ 上的 $G$ 的轨道数是

$$Z_G(b,b,\cdots,b)=\frac{1}{|G|}\sum_{\sigma\in G}b^{z_1(\sigma)+z_2(\sigma)+\cdots+z_n(\sigma)},$$

这里 $b:=|B|$.

**例 37.1** $n$ 阶循环群 $C_n$ 对 $n$ 的每个除数(或因子)$d$ 有 $\varphi(d)$ 个阶为 $d$ 的元素．作为 $C_n$ 的正则表示中的一个置换，阶为 $d$ 的一个元素有 $n/d$ 个长度为 $d$ 的圈．于是，对 $C_n$ 的正则表

示，我们有

$$Z_{C_n}(X_1,\cdots,X_n)=\frac{1}{n}\sum_{d|n}\varphi(d)X_d^{n/d}.$$

现在我们对两种颜色的 $n$ 个珠子做成的"单侧"项链的数目进行计数. 答案是 $Z_{C_n}(2,2,\cdots,2)=\frac{1}{n}\sum_{d|n}\varphi(d)2^{n/d}$；参见等式(10.12). 对 $n=6$，我们得到 14，比具有二面体等价性的多 1(此时(37.1)中的两个项链是不同的). 对 $n=10$，我们得到 108.

**例 37.2** 要找出 $n$ 个点上的通常表示的二面体群 $D_n$ 的圈指标，必须说明 $n$ 阶循环子群之外的置换(反射). 依据 $n$ 的奇偶性有两种情形：

525

$$Z_{D_n}=\begin{cases}\frac{1}{2n}\Big(\sum_{d|n}\varphi(d)X_d^{n/d}+nX_1X_2^{\frac{n-1}{2}}\Big) & n\text{ 为奇数},\\ \frac{1}{2n}\Big(\sum_{d|n}\varphi(d)X_d^{n/d}+\frac{n}{2}X_1^2X_2^{\frac{n}{2}-1}+\frac{n}{2}X_2^{\frac{n}{2}}\Big) & n\text{ 为偶数}.\end{cases}$$

用两种不同颜色的 $n$ 个珠子做成的"双侧"项链的数目是 $Z_{D_n}(2,2,\cdots,2)$. 对 $n=6$，我们得到 13(证实问题 1 之后的列表). 对 $n=10$，我们得到 78.

**问题 37A** 计算立方体的旋转群的圈指标，群由六个面的排列表示. (有 24 种旋转——包括恒同——把作为 3 维空间中的立方体映射到它自身. 忽略立方体的 24 个反射.)分别用 2 种颜色、3 种颜色、$n$ 种颜色给立方体的面染色，本质上不同的方法有多少?

进一步讨论之前，先写出对称群的圈指标. 注意在等式(13.3)中，一个给定类型$(1^{k_1}2^{k_2}\cdots n^{k_n})$的分拆数公式. 每个大小为 $i$ 的块能用$(i-1)!$ 种方法配备一个循环置换，于是我们有

$$Z_{S_n}=\sum_{(1^{k_1}2^{k_2}\cdots)}\frac{1}{1^{k_1}2^{k_2}\cdots n^{k_n}k_1!k_2!\cdots k_n!}X_1^{k_1}X_2^{k_2}\cdots X_n^{k_n}.$$

列出前面的几个多项式如下：

$$1!Z_{S_1}=X_1,$$

$$2!Z_{S_2}=X_1^2+X_2,$$

$$3!Z_{S_3}=X_1^3+3X_1X_2+2X_3,$$

$$4!Z_{S_4}=X_1^4+6X_1^2X_2+3X_2^2+8X_1X_3+6X_4,$$

$$5!Z_{S_5}=X_1^5+10X_1^3X_2+15X_1X_2^2+20X_1^2X_3+20X_2X_3+30X_1X_4+24X_5,$$

$$6!Z_{S_6}=X_1^6+15X_1^4X_2+45X_1^2X_2^2+40X_3^2+40X_1^3X_3+15X_2^3$$
$$+120X_1X_2X_3+90X_1^2X_4+90X_2X_4+144X_1X_5+120X_6.$$

**例 37.3** 定理 37.1 可用于图的计数. 设 $V$ 为一个 $n$ 个顶点的固定集合，再设 $E$ 由 $V$ 的所有 2-子集构成. 则顶点集为 $V$ 上的简单图可以视为映射 $f:E\to\{0,1\}$，对应于 $f$ 的图具有边集 $f^{-1}(1)=\{e:f(e)=1\}$.

526

$V$ 上的两个图是同构的，当且仅当存在 $V$ 的一个置换把一个图的边映成另一个图的边. 为

了把以上描述成适合应用定理 37.1 的形式，设 $S_n$ 为 $V$ 上的对称群，并设 $S_n^{(2)}=\{\sigma^{(2)}:\sigma\in S_n\}$ 是 $E$ 的置换的诱导群，同构于 $S_n$，这里

$$\sigma^{(2)}:\{x,y\}\mapsto\{\sigma(x),\sigma(y)\}.$$

则 $S_n^{(2)}$ 作用于$\{0,1\}^E$上，并且我们注意到 $f,g:E\to\{0,1\}$对应同构的图，当且仅当它们对于作用于$\{0,1\}^E$上的 $S^{(2)}$ 有相同的轨道.

计算 $S_n^{(2)}$ 中所有置换的类型不是一个轻松的任务. 例如，如果 $\sigma\in S_5$ 具有类型$(2^13^1)$，那么它产生的 $\sigma^{(2)}$ 在 $K_5$ 的 10 条边上有类型$(1^13^16^1)$. $S_5^{(2)}$ 的圈指标是

$$\frac{1}{120}(X_1^{10}+10X_1^4X_2^3+15X_1^2X_2^4+20X_1X_3^3+20X_1X_3X_6+30X_2X_4^2+24X_5^2).$$

一般地，我们将得到 $n$ 的所有分拆的和. 用 2 代替所有的变量，可以发现有 5 个顶点的不同构的图的数目是 34.

现在，把定理 37.1 推广到允许有重量的情形. 设 $A$ 为一个 $n$-集合，$G$ 作用于 $A$ 上，并设 $B$ 是颜色的一个有限集. 设 $R$ 是一个包含有理数的交换环，设 $w:B\to R$ 对每种颜色 $b\in B$ 赋予一个重量 $w(b)\in R$. 对 $f:A\to B$，定义

$$W(f):=\prod_{a\in A}w(f(a))\in R;$$

这里 $W(f)$是函数 $f$ 的重量. 注意，表示 $G$ 作用于 $B^A$ 上的同一轨道的两个映射有相同的重量，即对所有的 $\sigma\in G$，$W(\sigma(f))=W(f)$. 和

$$\sum_{f\in R}W(f)$$

527

遍及轨道的代表系 $R$，称为*构形计数级数*(轨道常常称为*构形*；当重量是单项式时，术语级数才恰当.)如果所有的重量 $w(b)$都等于 1，下面的定理化为定理 37.1.

**定理 37.2** *用上面的术语，构形计数级数由*

$$\sum W(f)=Z_G\Big(\sum_{b\in B}w(b),\sum_{b\in B}[w(b)]^2,\cdots,\sum_{b\in B}[w(b)]^n\Big)$$

*给出.*

**证明** 设 $N=\sum W(f)$，和遍及 $\sigma\in G$，$f\in B^A$ 且 $\sigma(f)=f$ 的所有对$(\sigma,f)$. 我们有

$$N=\sum_{f\in B^A}W(f)\mid G_f\mid,$$

其中 $G_f$ 是 $f$ 的稳定化子. 把项 $W(f)\mid G_f\mid$ 看成 $f$ 遍及 $G$ 作用在 $B^A$ 上的一条轨道$\mathcal{O}$：每一项等于 $W(f_0)\mid G\mid/\mid\mathcal{O}\mid$，这里 $f_0$ 是轨道$\mathcal{O}$的一个表示，于是这些项的和等于 $\mid G\mid W(f_0)$. 现在，很显然 $N$ 等于 $\mid G\mid$ 乘以构形计数级数.

另一方面，

$$N=\sum_{\sigma\in G}\Big(\sum_{\sigma(f)=f}W(f)\Big).$$

回忆 $Z_G$ 的定义，可以看到如果我们能证明

$$\sum_{\sigma(f)=f}W(f)=\Big(\sum_{b\in B}w(b)\Big)^{k_1}\Big(\sum_{b\in B}[w(b)]^2\Big)^{k_2}\cdots\Big(\sum_{b\in B}[w(b)]^n\Big)^{k_n},$$

只要 $\sigma$ 是类型为$(1^{k_1}2^{k_2}\cdots n^{k_n})$的一个置换，就完成了证明.

一个映射 $f: A\to B$ 被 $\sigma$ 固定，当且仅当 $f$ 在 $\sigma$ 作用于 $A$ 的每个圈上是常数. 设

528

$$C_1, C_2, \cdots, C_k, \quad k := k_1 + k_2 + \cdots + k_n$$

是 $\sigma$ 的圈. 由 $\sigma$ 固定的映射 $f\in B^A$ 与 $B$ 的元素的 $k$ 元组$(b_1, b_2, \cdots, b_k)$一一对应(对应映射是把 $b_i$ 与 $C_i$ 的所有元素联系起来). 对应于$(b_1, \cdots, b_k)$的映射 $f$ 的重量是

$$W(f) = \prod_{i=1}^{k}[w(b_i)]^{|C_i|},$$

并对所有的 $k$ 元组$(b_1, b_2, \cdots, b_k)$求和，

$$\begin{aligned}\sum_{\sigma(f)=f} W(f) &= \sum_{b_1, b_2, \cdots, b_k}[w(b_1)]^{|C_1|}[w(b_2)]^{|C_2|}\cdots[w(b_k)]^{|C_k|} \\ &= \Big(\sum_{b_1}[w(b_1)]^{|C_1|}\Big)\Big(\sum_{b_2}[w(b_2)]^{|C_2|}\Big)\cdots \\ &= \prod_{c=1}^{n}\Big(\sum_{b}[w(b)]^{c}\Big)^{k_c},\end{aligned}$$

正如所要求的. ■

**例 37.4** 考虑循环等价的项链问题. 这里 $G=C_n$，$B=\{$黑，白$\}$. 我们取 $R$ 为多项式环 $\mathbb{Q}[X]$，定义 $w($黑$)=1$，$w($白$)=X$. 染色 $f: A\to B$ 的重量是

$$W(f) = X^k,$$

其中 $k$ 是白珠子的数目.

于是，$n$ 个珠子(其中 $k$ 个是白珠子)的本质上不同的环状项链的数目是构形计数级数

$$\begin{aligned}&Z_{C_n}(1+X, 1+X^2, 1+X^3, \cdots, 1+X^n) \\ &= \frac{1}{n}\sum_{d|n}\varphi(d)[1+X^d]^{n/d} \\ &= \frac{1}{n}\sum_{d|n}\varphi(d)\sum_{r=0}^{n/d}\binom{n/d}{r}x^{rd}\end{aligned}$$

529

中 $X^k$ 的系数. 这个系数是

$$\frac{1}{n}\sum_{d|(k,n)}\varphi(d)\binom{n/d}{k/d}.$$

因此，如果 $k$ 和 $n$ 互素，这个数目仅仅是 $\frac{1}{n}\binom{n}{k}$，当 $n=12$，$k=4$ 时，有 $\frac{1}{12}\Big(\varphi(1)\binom{12}{4}+\varphi(2)\binom{6}{2}+\varphi(4)\binom{3}{1}\Big)=43$ 种项链.

**问题 37B** 给一个立方体的面染色，使得一个面是红色，两个面是蓝色，并且其余的三个面是绿色. 本质上不同的染色方法数是多少? 分别用手工运算(这也许更快)和定理 37.2 来做，并比较你的答案.

设 $A$ 和 $B$ 为有限集，$|A|=n$，又设 $G$ 和 $H$ 为有限群，$G$ 作用在 $A$ 上且 $H$ 作用在 $B$ 上. 直积 $G\times H$ 作用在 $B^A$ 上，当 $f\in B^A$ 且$(\sigma, \tau)\in G\times H$ 时，用

$$((\sigma,\tau)(f))(a) = \tau(f(\sigma^{-1}(a)))$$

定义$(\sigma, \tau)(f)$.

**定理 37.3**　$G\times H$ 作用在 $B^A$ 上的轨道数是

$$\frac{1}{|H|}\sum_{\tau\in H} Z_G(m_1(\tau), m_2(\tau), \cdots, m_n(\tau)),$$

其中

$$m_i(\tau) := \sum_{j|i} j z_j(\tau), \quad i = 1,2,\cdots,n.$$

**证明**　由伯恩赛德引理，轨道数是

$$\frac{1}{|G||H|}\sum_{\sigma\in G,\tau\in H}\psi(\sigma,\tau),$$

这里 $\psi(\sigma, \tau)$是使得$(\sigma, \tau)(f)=f$ 的映射 $f\in B^A$ 的数目. 为了完成证明，对每个 $\tau\in H$，证明

$$\frac{1}{|G|}\sum_{\sigma\in G}\psi(\sigma,\tau) = Z_G(m_1(\tau), m_2(\tau), \cdots, m_n(\tau)) \tag{37.3}$$

就够了.

530

固定 $\sigma\in G$ 和 $\tau\in H$，并设

$$C_1, C_2, \cdots, C_k, \quad k := z_1(\sigma) + z_2(\sigma) + \cdots + z_n(\sigma)$$

是 $\sigma$ 在 $A$ 上的圈. 一个映射 $f: A\to B$ 被$(\sigma, \tau)$固定，当且仅当所有的限制 $f_i := f\mid C_i(1\leqslant i\leqslant k)$ 是固定的. 于是 $\psi(\sigma, \tau)$是满足

$$f_i(\sigma(a)) = \tau(f_i(a)) \quad 对所有的\ a\in C_i$$

的映射 $f_i: C_i\to B$ 的数目的乘积，$i$ 的范围是 $1\leqslant i\leqslant k$.

设 $C_i$ 有长度 $\ell$ 并固定 $a_o\in C_i$. 假设 $f_i: C_i\to B$ 被$(\sigma\mid C_i, \tau)$固定并且 $f_i(a_o)=b$. 则 $f_i$ 完全被确定：$f_i(\sigma^t(a_o))=\tau^t(b)$. 此外，$b=f_i(a_o)=f_i(\sigma^\ell(a_o))=\tau^\ell(b)$，因此我们看到 $\tau$ 的包含 $b$ 的圈一定有长度 $\ell'$，$\ell'$是 $\ell$ 的因子.

反之，如果 $b$ 是 $B$ 的一个位于 $\tau$ 的圈上的元素，圈的长度整除 $\ell := |C_i|$，那么我们可以在 $C_i$ 上由 $f_i(\sigma^t(a_o)) := \tau^t(b)$定义一个映射 $f_i$(检查 $f_i$ 是有良好定义的)，而且这个 $f_i$ 被$(\sigma\mid C_i, \tau)$固定.

总之，当 $|C_i|=\ell$ 时，固定的映射 $f_i: C_i\to B$ 在数目上与 $B$ 的位于 $\tau$ 的长度整除 $\ell$ 的圈中的元素相等. 当然，这样的元素数是

$$m_\ell(\tau) = \sum_{j|\ell} j z_j(\tau).$$

则

$$\psi(\sigma,\tau) = \prod_{i=1}^{k} m_{|C_i|}(\tau) = [m_1(\tau)]^{z_1(\sigma)}[m_2(\tau)]^{z_2(\sigma)}\cdots[m_n(\tau)]^{z_n(\sigma)},$$

由此立即得到想要的等式(37.3). ■

**例 37.5**　把 2 个红球、2 个黄球和 4 个绿球放在 1 个圆盒子和 3 个方盒子中的方法数是多少？我们取

$$A = \{R_1, R_2, Y_1, Y_2, G_1, G_2, G_3, G_4\},$$

531

$$G = S_2 \times S_2 \times S_4, \quad B = \{r, s_1, s_2, s_3\}, \quad H = S_1 \times S_3.$$

容易看出 $G$ 的圈指标是对称群的圈指标的积，$G$ 是对称群之积，因此

$$\begin{aligned} Z_G &= Z_{S_2} \cdot Z_{S_2} \cdot Z_{S_4} \\ &= \frac{1}{2!2!4!}(X_1^2 + X_2)^2(X_1^4 + 6X_1^2X_2 + 3X_2^2 + 8X_1X_3 + 6X_4). \end{aligned} \tag{37.4}$$

在 $H$ 中有三种类型的置换. 如果 $\tau$ 是恒等置换，则

$$m_1(\tau) = 4, \quad m_2(\tau) = 4, \quad m_3(\tau) = 4, \quad m_4(\tau) = 4;$$

如果 $\tau$ 互换$\{s_2, s_2, s_3\}$中的两个，则

$$m_1(\tau) = 2, \quad m_2(\tau) = 4, \quad m_3(\tau) = 2, \quad m_4(\tau) = 4;$$

如果 $\tau$ 只固定 $r$，则

$$m_1(\tau) = 1, \quad m_2(\tau) = 1, \quad m_3(\tau) = 4, \quad m_4(\tau) = 1.$$

由定理 37.3，方法数是

$$\begin{aligned} &\frac{1}{3!}\frac{1}{2!2!4!}[(4^2+4)^2(4^4+6\cdot 4^2\cdot 4+2\cdot 4^2+8\cdot 4\cdot 4+6\cdot 4) \\ &+3(2^2+4)^2(2^4+6\cdot 2^2\cdot 4+3\cdot 4^2+8\cdot 2\cdot 2+6\cdot 4) \\ &+2(1^2+1)^2(1^4+6\cdot 1^2\cdot 1+3\cdot 1^2+8\cdot 1\cdot 4+6\cdot 1)] \\ &= 656(\text{如果我们的算术运算无误的话}). \end{aligned}$$

**问题 37C** 给定 $G$ 作用在 $A$ 上，$H$ 作用在 $B$ 上，求单射 $f: A \to B$ 的轨道数的表达式.

我们不加证明地给出定理 37.3 扩充到含重量情形的陈述. 证明见 De Bruijn(1964). 如果所有的重量都等于 1，这个定理化为定理 37.3.

**定理 37.4** *假设 $G$ 作用在 $A$ 上，$H$ 作用在 $B$ 上，设 $R$ 为一个交换环且 $w: B \to R$. 假设 $w$ 在 $H$ 作用在 $B$ 上的每个轨道中是常数. 由 $W(f) := \prod_{a \in A} w[f(a)]$，遍及 $G \times H$ 作用于 $B^A$ 上的轨道的一个代表系的和 $\sum W(f)$ 等于*

532

$$\frac{1}{|H|}\sum_{\tau \in H} Z_G(M_1(\tau), M_2(\tau), \cdots, M_n(\tau)),$$

*这里*

$$M_i(\tau) = \sum_{\tau^i(b)=b} [w(b)]^i.$$

**例 37.6** 我们继续例 13.5. 取

$$w(r) = r, \quad w(s_1) = w(s_2) = w(s_3) = s,$$

这里 $R = \mathbb{Q}[r, s]$. $t$ 个球放到圆盒子中且其余 $8-t$ 个球放到方盒子中的方法数是

$$\begin{aligned} &\frac{1}{6}\Big(Z_G(r+3s, r^2+3s^2, r^3+3s^3, r^4+3s^4) \\ &+3Z_G(r+s, r^2+3s^2, r^3+s^3, r^4+3s^4)+2Z_G(r, r^2, r^3+3s^3, r^4)\Big) \end{aligned}$$

中 $r^ts^{8-t}$ 的系数，这里 $Z_G$ 是在(37.4)中的那个多项式.

**问题 37D** 把有染色珠子的两种类型的项链与通过交换颜色而得到的对偶等同.（现在我

们能区分两种颜色，但不能说明哪一个是哪一个.）有多少这样约化过的构形？（例如，由 $n=6$ 和二面体等价性，有 8 种不同的构形.）有多少项链是自对偶的？

**问题 37E** 用 $s$ 种颜色给立方体的面染色，$t$ 种颜色给它的顶点染色（假定用于面的颜色和用于顶点的颜色不同，尽管这不重要）. 有多少种本质上不同的方法（相对于立方体的旋转群）？

* * *

本章的诸定理也是代数恒等式的源泉. [533]

考虑“把相同的对象放到不同的腔中”这一情形.（回忆第 13 章中讨论过的一些内容.）例如，有多少种方法把 23 个苹果分给张三、李四和王五？更一般地，考虑把 $n$ 个苹果的一个集合 $A$ 分给 $x$ 个人的一个集合 $B$（$A$ 中的元素是“相同的”，同时 $B$ 中的元素是不同的）的分法. 这样的分法相当于选择一组非负整数 $k_b(k_b: b\in B)$ 使 $\sum_{b\in B}k_b=n$，人 $b$ 分得 $k_b$ 个苹果.

于是分法数（如定理 13.3 中的证明）是

$$\binom{n+x-1}{n}.$$

然而，这样的分法在形式上最好是作为对称群 $S_n$ 作用于 $A$ 的映射 $f: A\to B$ 的轨道定义.（两个映射 $f$，$g\in B^A$ 确定相同的分法，当且仅当它们的苹果排列“不同”.）由定理 37.1，分法数是

$$\frac{1}{n!}\sum_{k=0}^{n}c_k(S_n)x^k,$$

这里 $c_k(S_n)$ 是 $n$ 个字母的恰有 $k$ 个圈的排列数. 在第 13 章中，数 $c_k(S_n)$ 称为无符号的第一类斯特林数，并用 $c(n, k)$ 表示. 由定理 37.2，对每个非负整数 $x$，

$$(x+n-1)_{(n)}=\sum_{k=0}^{n}c_k(S_n)x^k,$$

因此作为一个多项式恒等式它必定成立. 我们再次证明了公式(13.7).

取 $G$ 为作用在一个 $n$-集合 $A$ 上的 $S_n$，设 $B$ 是有限的且设 $w$ 是 $B$ 在多项式环 $\mathbb{Q}[B]$ 中的插入. 这里映射 $f: A\to B$ 的重量是一个单项式并且两个映射是等价的，即表示同一个构形，当且仅当它们有相同的重量. 构形计数级数 [534]

$$\sum W(f)=Z_{S_n}\Big(\sum_{b\in B}b,\sum_{b\in B}b^2,\cdots,\sum_{b\in B}b^n\Big) \tag{37.5}$$

把所谓的齐次-积-和对称函数表示成一个幂-和对称函数的多项式. 例如，对 $n=3$ 且 $B=\{X, Y\}$，

$$\begin{aligned}&6(X^3+X^2Y+XY^2+Y^3)\\&=(X+Y)^3+3(X+Y)(X^2+Y^2)+2(X^3+Y^3).\end{aligned}$$

对 $n=4$ 且 $B=\{X, Y, Z\}$，(37.5)把

$$\sum_{i+j+k=4}X^iY^jZ^k$$

表示成一个 $X+Y+Z$，$X^2+Y^2+Z^2$，$X^3+Y^3+Z^3$ 和 $X^4+Y^4+Z^4$ 的多项式.

## 评注

我们谈及 $Z_{S_n}(X_1, \cdots, X_n)$是$(\mathbb{Q}[X_1, X_2, \cdots])[[Y]]$的一个元素

$$\exp\left(X_1Y+\frac{1}{2}X_2Y^2+\frac{1}{3}X_3Y^3+\cdots\right)$$

中 $Y^n$ 的系数.

波利亚理论给出的解答的一个优势(比如说，与容斥原理相比)是公式中出现的是正项的和而不是正负交错项的和.

波利亚(G. Pólya，1887—1985)是匈牙利数学家，他与 G. Szegö 在 1924 年合著的《Problems and Theorems in Analysis》仍然是一本经典. 但是，也许他广为人知的书是《How to Solve It》，这本书售出了超过一百万册. 他的论文涉及数论、复分析、组合学、概率论、几何学和数学物理领域.

## 参考文献


N. G. de Bruijn (1964), Pólya's theory of counting, in: E. F. Beckenbach (ed.), *Applied Combinatorial Mathematics*, Wiley.

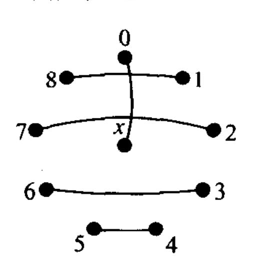
F. Harary and E. D. Pulver (1966), The power group enumeration theorem, *J. Combinatorial Theory* **1**.


535

# 第38章 Baranyai定理

在这一章中，我们给出关于流的整数性定理在“组合设计”中一个问题上的精彩应用.

**例 38.1** 假定我们受委托为10支足球队拟一个日程表. 每个周末将它们分成5对踢球. 在9周结束时，让每个可能的一对球队恰好踢球一次.



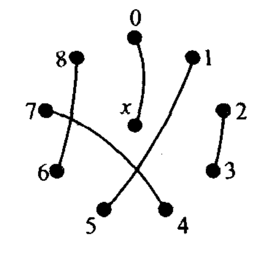

这里是一个解. 把9支球队放在一个正九边形的顶点上，一个球队放在它的中心. 以右图所示的配对开始并通过把图形转动 $2\pi/9$ 的倍数得到其他配对.

下面是明显的日程表：

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $x$ •-• 0 | $x$ •-• 1 | $x$ •-• 2 | $x$ •-• 3 | $x$ •-• 4 | $x$ •-• 5 | $x$ •-• 6 | $x$ •-• 7 | $x$ •-• 8 |
| 1 •-• 8 | 2 •-• 0 | 3 •-• 1 | 4 •-• 2 | 5 •-• 3 | 6 •-• 4 | 7 •-• 5 | 8 •-• 6 | 0 •-• 7 |
| 2 •-• 7 | 3 •-• 8 | 4 •-• 0 | 5 •-• 1 | 6 •-• 2 | 7 •-• 3 | 8 •-• 4 | 0 •-• 5 | 1 •-• 6 |
| 3 •-• 6 | 4 •-• 7 | 5 •-• 8 | 6 •-• 0 | 7 •-• 1 | 8 •-• 2 | 0 •-• 3 | 1 •-• 4 | 2 •-• 5 |
| 4 •-• 5 | 5 •-• 6 | 6 •-• 7 | 7 •-• 8 | 8 •-• 0 | 0 •-• 1 | 1 •-• 2 | 2 •-• 3 | 3 •-• 4 |

有多种方法可用来排日程表. 例如，以右图所示的初始配对开始的方法.

536




图中的一个完美匹配也称为1-因子. 一个图的边集的1-因子划分也称为1-因子分解. 在上面的例子中，构造了 $K_{10}$ 的1-因子分解. $K_{10}$ 有396个不同构的1-因子分解，这是 E. N. Gelling(1973)由计算机得到的结果. 也见 Mendelsohn and Rosa(1985).

**例 38.2** 设 $\Gamma$ 是奇阶的交换群. 考虑顶点集 $\Gamma\cup\{\infty\}$ 上的一个完全图. 对 $g\in\Gamma$，设

$$\mathcal{M}_g := \{\{g,\infty\}\}\cup\{\{a,b\}: a+b=2g, a\neq b\}.$$

则 $\{\mathcal{M}_g : g\in\Gamma\}$ 是这一完全图的一个1-因子分解.

我们考虑这个问题的如下推广：用一个 $n$-集合的 $k$-子集的平行类这个术语指有 $n/k$ 个 $k$-子集的一个集合划分 $n$-集合. 所有 $k$-子集的集合能划分成 $k$-子集的平行类吗？当然，$k$ 整除 $n$ 是必需的. 所需平行类的数目是 $\frac{k}{n}\binom{n}{k}=\binom{n-1}{k-1}$.

这个问题对 $k=2$ 并不难. 但对1936年 R. Peltesohn 所做的 $k=3$ 和 J.-C. Bermond 所做的 $k=4$(未发表)要难得多. 对 $n=9$ 和 $k=3$，读者可试着找出合适的平行类. 由于的确不知道我们的推广总有一个解，因此当 Zs. Baranyai 在1973年证明定理38.1时非常令人惊奇. 所有已知的证明都利用了定理7.2或定理7.4的一种形式或结论. 我们给出的证明属于 A. E. Brouwer and A. Schrijver(1979).

**定理 38.1** 如果 $k$ 整除 $n$，则一个 $n$-集合的所有 $\binom{n}{k}$ 个 $k$-子集的集合可以划分成不相交的平行类 $\mathcal{A}_i$，$i=1, 2, \cdots, \binom{n-1}{k-1}$.

**证明** 在这个证明中，用一个集合 $X$ 的 $m$-划分指 $X$ 的 $m$ 个两两不相交的子集的一个多重集 $\mathcal{A}$，其中有些可能是空的，它们的并等于 $X$.（对“划分”的正常使用不允许有空集，但在这里允许有空集是很重要的，也许由于重数，使子集的总数是 $m$.）

537

为了使归纳证明有效，我们证明似乎比原来的断言强的结论．设给定 $n$ 和 $k$，假设 $k$ 整除 $n$，并设 $m:=n/k$，$M:=\binom{n-1}{k-1}$．我们断言：对任何整数 $\ell$，$0\leqslant\ell\leqslant n$，存在$\{1,2,\cdots,\ell\}$的 $m$-划分的一个集合

$$\mathcal{A}_1,\mathcal{A}_2,\cdots,\mathcal{A}_M,$$

它具有以下性质：每个子集 $S\subseteq\{1,2,\cdots,\ell\}$在 $m$-划分 $\mathcal{A}_i$ 中恰出现

$$\binom{n-\ell}{k-|S|} \tag{38.1}$$

次．（当然，上面的二项式系数当 $|S|>k$ 时取 0，且对 $S=\varnothing$，包含$\varnothing$的 $m$-划分按重数计数等于空集出现的次数．）

我们的断言由对 $\ell$ 进行归纳证明．注意当 $\ell=0$ 时，每个 $\mathcal{A}_i$ 由空集的 $m$ 个拷贝组成，断言显然正确．还注意到，当 $\ell=n$ 时定理 38.1 得证，因为此时(38.1)中的二项式系数是

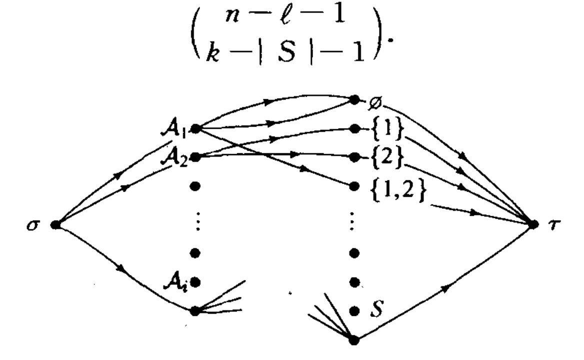
$$\binom{0}{k-|S|}=\begin{cases}1 & \text{如果 } |S|=k,\\ 0 & \text{否则}.\end{cases}$$

**注记** 这个稍专门化的断言实际上并不比原始断言更通用，但容易从定理 38.1 得出．如果如同定理 38.1 的断言，$M$ 个平行类存在，那么对 $X$ 的 $\ell$ 个点的任意一个集合 $L$，平行类中的成员与 $L$ 的交提供了具有上述性质的 $L$ 的 $m$-划分．

假定对某个值 $\ell<n$，存在 $m$-划分 $\mathcal{A}_1,\cdots,\mathcal{A}_M$ 具有所要求的性质．我们如下建立一个运输网络．有一个发点 $\sigma$，对每个 $i=1,2,\cdots,M$ 的名为 $\mathcal{A}_i$ 的顶点，对每个子集 $S\subseteq\{1,2,\cdots,\ell\}$ 的名为 $S$ 的顶点，以及一个收点 $\tau$．从 $\sigma$ 到每个 $\mathcal{A}_i$ 有容量为 1 的一条有向边．从 $\mathcal{A}_i$ 到 $\mathcal{A}_i$ 的成员对应的顶点有有向边(利用到$\varnothing$的 $j$ 条边，如果$\varnothing$在 $\mathcal{A}_i$ 中出现 $j$ 次)；这些边可以有$\geqslant1$ 的任意整数容量．从与一个子集 $S$ 对应的顶点到 $\tau$ 的一条有向边具有容量

538

$$\binom{n-\ell-1}{k-|S|-1}.$$




下面展示这个网络中的一个流：对离开 $\sigma$ 的边赋予 1 的流值，对从 $\mathcal{A}_i$ 到它的成员 $S$ 中的每一个的那些边赋予$(k-|S|)/(n-\ell)$的流值，对从 $S$ 到 $\tau$ 赋予$\binom{n-\ell-1}{k-|S|-1}$的流值．容易验证这是一个流：离开顶点 $\mathcal{A}_i$ 的边上的值之和是

$$\sum_{S\in\mathcal{A}_i}\frac{k-|S|}{n-\ell}=\frac{1}{n-\ell}\Big(mk-\sum_{S\in\mathcal{A}_i}|S|\Big)=\frac{1}{n-\ell}(mk-\ell)=1.$$

进入顶点 $S$ 的边上的值之和是

$$\sum_{i:S\in\mathcal{A}_i}\frac{k-|S|}{n-\ell}=\frac{k-|S|}{n-\ell}\binom{n-\ell}{k-|S|}=\binom{n-\ell-1}{k-|S|-1}.$$

因为离开 $\sigma$ 的所有边是饱和的，这是一个最大流且具有强度 $M$．进入 $\tau$ 的边在这个流中也是饱

和的，且因此在任何一个最大流中是饱和的. [539]

由定理 7.2，这个网络容许一个整数值的最大流 $f$. 离开 $\sigma$ 的所有边是饱和的，于是对每个 $i$，显然 $f$ 对离开 $\mathcal{A}_i$ 中的边之一赋予值 1，对所有其他的边赋予值 0. 比如说 $f$ 对从 $\mathcal{A}_i$ 到它的成员 $S_i$ 的边赋予值 1. 对每个子集 $S$，使得 $S_i=S$ 的 $i$ 值的数目是 $\binom{n-\ell-1}{k-|S|-1}$.

(不用显式地引入容量而利用定理 7.2 也能得到想要的整数流 $f$，简单地应用定理 7.4，通过添加从 $\tau$ 到 $\sigma$ 的流值为 $M$ 的一条边，显示有理流闭合而成为环流即可.)

最后，通过从 $\mathcal{A}_i$ 中由 $S_i\cup\{\ell+1\}(i=1,\cdots,M)$ 替换显著成员 $S_i$ 而得到 $\mathcal{A}_i'$，我们获得集合 $\{1,2,\cdots,\ell+1\}$ 的 $m$-划分 $\mathcal{A}_1',\cdots,\mathcal{A}_M'$ 的一个集合. 读者应检查 $\{1,2,\cdots,\ell+1\}$ 的每个子集 $T$ 在 $\mathcal{A}_1',\cdots,\mathcal{A}_M'$ 中恰出现

$$\binom{n-(\ell+1)}{k-|T|}$$

次. 这就完成了归纳步骤. ■

**问题 38A** 设 $v$ 和 $u$ 是两个整数，$v\geqslant 2u$ 且 $v$ 为偶数，完全图 $K_u$ 作为 $K_v$ 的一个子图考虑. 假设 $K_u$ 的边用 $v-1$ 种色染色，使得同种色的不同边不相交. 证明：这种染色可以扩展到用 $v-1$ 种色对 $E(K_v)$ 的染色，使得同色的边不相交. ($E(K_v)$ 的这一染色等价于 $K_v$ 的 1-因子分解，染任意给定的一种颜色的边构成一个 1-因子.)

## 评注

Zsolt Baranyai(1948—1978)是匈牙利数学家，也是一位专业的录音师. 他在随 Barkfark Consort 巡回举行音乐会期间因车祸丧生. 他的数学工作包括许多关于"完全均匀超图"的出色结果.

完全图的 1-因子分解与对称拉丁方有关——参见第 17 章. 问题 38A 的结果属于 Cruse (1974). 推广可在 Baranyai and Brouwer(1977)中找到. [540]

## 参考文献


Zs. Baranyai and A. E. Brouwer (1977), Extension of colourings of the edges of a complete (uniform hyper) graph, *Math. Centrum Dep. Pure Math. ZW.* **91**, 10 pp.

A. E. Brouwer and A. Schrijver (1979), Uniform hypergraphs, in: A. Schrijver (ed.), *Packing and Covering in Combinatorics*, Mathematical Centre Tracts **106**, Amsterdam.

A. Cruse (1974), On embedding incomplete symmetric Latin squares, *J. Combinatorial Theory* (A) **16**, 18–22.

E. N. Gelling (1973), On 1-factorizations of the complete graph and the relationship to round robin schedules, M.Sc. Thesis, University of Victoria.

E. Mendelsohn and A. Rosa (1985), One-factorizations of the complete graph—a survey, *Journal of Graph Theory* **9**.

R. Peltesohn (1936), Das Turnierproblem für Spiele zu je dreien, Dissertation Berlin, August Pries, Leipzig. [541]

# 附录1　问题的提示和评论

**问题 1A**　证明来自{1，…，5}的$\binom{5}{2}$个数对可以如此给顶点标号：当存在一条边时，有一个简单的法则能予以确定．为了找到完全的自同构群，考虑固定一个顶点及其三个邻点的子群．这个图以彼得森图著称．该图首先由丹麦数学家 J. P. C. Petersen(1839—1910)研究．也见第 21 章．

**问题 1B**　设顶点集 $V$ 是 $V_1$ 和 $V_2$ 的不相交的并，且没有从 $V_1$ 到 $V_2$ 的边．边的可能的最大数目是多少？

**问题 1C**　利用(1.1)．(i)考虑一个 1 次的顶点；用归纳法．(ii)回路的边数与顶点数相同；如果图是连通的，每个顶点的次≥1.

**问题 1D**　称顶点为 $a_1$，$a_2$，$a_3$ 以及 $b_1$，$b_2$，$b_3$．首先，忽略 $a_3$ 并证明在平面上只有一种方式画出其余 6 条边的图．更好的途径是使用欧拉公式(参见第 33 章)．

**问题 1E**　在一个回路上每种颜色出现偶数次．参见 J. A. Bondy，Induced subsets，*J. Combinatorial Theory*(B)12(1972)，201-202．这个问题也可陈述如下．给定一个有不同行的(0，1)-方阵，可以删去一列使得到的矩阵的行不相同．这一事实易于由归纳法证明．

542

**问题 1F**　考虑离一个固定的顶点距离为 2 的顶点．参见图 1.4.

**问题 1G**　利用鸽巢原理．

**问题 1H**　考虑 $a_{ij}=a_{jk}=1$ 的情形．

**问题 1I**　对构造所要求的回路找出归纳步骤．

**问题 1J**　对(i)，在 $x$ 相邻的顶点和 $y$ 相邻的顶点之间建立一个一一对应．

**问题 2A**　22335 的任何一个排列均可．

**问题 2C**　设 $A_i$ 是以 $x_i$ 为根的支撑树形图的数目，$r_i$ 表示从 $x_i$ 出来的边的数目．断言通过证明 $G$ 中不同的欧拉回路的数目为

$$A_i\prod_{j=1}^{n}(r_j-1)!$$

而得证．为此，取 $i=1$ 并考虑 $x_1$ 作为根的某个支撑树形图．固定从 $x_1$ 出来的某条边作为一个欧拉回路的第一条边．任意给从 $x_1$ 出来的其他边标号．对 $i=2，3，\cdots，n$，给从 $x_i$ 出来的边任意标号但使得支撑树形图的边的标号为 $r_i$．这种标号导致构造欧拉回路的自然方式且这一过程可以倒过来．参见 J. H. van Lint，*Combinatorial Theory Seminar*，*Eindhoven University of Technology* 的第 9 章，Lecture Notes in Mathematics 382，Springer-Verlag，1974.

**问题 2D**　一种途径如下．证明 $T_n$ 具有以下性质：对它的每一条边 $a$，$a$ 的端点在 $G:\{e\in E(G):c(e)<c(a)\}$的不同分支中．然后证明具有这一性质的任意支撑树 $T$ 是最便宜的支撑树．

**问题 2E**　只存在一种方式获得差 $n-1$，等等．

**问题 2F**　利用问题 1C.

**问题 2G** 如果 $G$ 是具有这种性质的图，证明存在具有相同性质、相同边数，且在图中次为 $m$ 的顶点与所有其他次 $>1$ 的顶点相连的图 $G'$. 然后用归纳法($m \to m+2$). 由相同的想法可归纳地作出图. 543

**问题 3A** 对(ii)，如果结论不正确，则 $H$ 可以写成两个边不交的子图 $A$，$B$ 的并，它们交于两个顶点 $s$，$t$. 对增加连结 $s$，$t$ 的边而分别由 $A$，$B$ 得到的 $A'$，$B'$用归纳假设.

**问题 3B** 利用与对 $K_6$ 给出的同一类型的论证(下一问题是可能的). 证明一定有一个顶点在两个单色三角形中. 然后，讨论其余的 6 个顶点. 论证既长且有技巧. 被误导的读者应了解定理 3.2 的推论.

**问题 3C** 称右边的两项(它们都是偶数)为 $n_1$ 和 $n_2$. 假定等号成立，考虑有 $n_1+n_2-1$ 个顶点的图. 如果不存在红色的 $K_p$ 和蓝色的 $K_q$，任意一个顶点的红色次数是多少? 在此图中红色的边有多少?

**问题 3D** 在$\mathbb{Z}_{17}$中考虑$\pm 2^i$，$i=0$，1，2，3. 对另一个问题考虑$\mathbb{Z}_{13}$. 应用(3.4).

**问题 3E** (a)固定一个顶点并分别考虑到这个顶点和离开这个顶点的所有边. 挑出较大的集合并用归纳法.

(b)利用概率方法. 在 P. Erdös and J. Spencer(1974)的定理 1.1 中可以找到一个解答，在那里这个问题用于描述概率方法.

**问题 3F** 顶点取作$\{1, 2, \cdots, n\}$. $\{i, j\}$染成 $|i-j|$. 为了避免两种颜色的三元组，如果 1 是红色，则 2 一定是蓝色且因此 4 一定是红色，等等. $N(2)=5$. 通过带第三种颜色的 5 个数分离出两个这样的 2-色构形，估计 $N(13)$. 参见 I. Schur，Über die Kongruenz $x^m+y^m\equiv z^m \pmod p$，*Jber. Deutsche Math. Ver.* 25(1916)，114-116.

**问题 3G** 以四种"颜色"如此染色：

$$\{i,j\} \mapsto (a_{ij}, a_{ji}) \quad (i<j).$$

544

**问题 3H** 利用对 $K_6$ 和两种颜色的论证.

**问题 3I** 设颜色依赖 $\nu \pmod 3$. 证明在$\mathbb{F}_{16}^{\star}$中两个立方体的和不是立方体.

**问题 3J** 考虑具有题目所要求的性质的极大子图，然后考虑不在这个子图中的顶点.

**问题 3K** 考虑颜色固定的顶点并删去使重新染色成为可能的边.

**问题 4A** (i)如此给 $K_{10}$ 染色，使得红色对应 $G$ 中的一条边，蓝色对应一条非边(nonedge). 存在三条边都是红色、两条边是红色且一条边是蓝色、两条边是蓝色且一条边是红色，以及三条边都是蓝色的三角形. 设 $a_i$($i=1$，2，3，4)是这些三角形的数目. 对这些数目建立一个由方程和不等式构成的系统，用 $G$ 的顶点的次表示. 这些式子表明在 $G$ 中至少有四个三角形，并且等式在此后可被排除，再查看其他方程.

(ii)另一种解法如下. 证明存在一个三角形. 然后考虑一个三角形、七元组的集合，以及两者之间的边. 这给出两种类型的新三角形的数目；估计这个数目.

**问题 4B** 利用归纳法. 首先复习一下定理 4.1 的证明.

**问题 4C** 在以 $x$ 和 $y$ 为端点的边 $a$ 上，三角形的数目至少为 $\deg(x)+\deg(y)-n$. 对此在所有的边 $a$ 上求和.

**问题 4D** 固定任意顶点 $x$，再设 $D_i$ 为 $G$ 中离 $x$ 的距离为 $i$ 的顶点的集合.

对 $g=2t+1$，因为对 $i=1, 2, \cdots, t$ 容易看出 $|D_i|=r(r-1)^{i-1}$，因此 $|V(G)|\geqslant 1+r+r(r-1)+\cdots+r(r-1)^{t-1}$.

对 $g=2t$，对 $i=1, 2, \cdots, t-1$，仍然有 $|D_i|=r(r-1)^{i-1}$. 我们也能得到一个下界 $|D_t|\geqslant\frac{r-1}{r}D_{t-1}$，因为每个顶点 $y\in D_{t-1}$ 在 $D_t$ 中与 $r-1$ 个顶点相邻，同时顶点 $y\in D_t$ 在 $D_{t-1}$ 中当然至多与 $r$ 个顶点相邻.

**问题 4E** 该图是二部图.

545

**问题 4F** 由定理 4.3，存在一个哈密顿回路 $H$. 假定 $H$ 不含端点为 $x$ 和 $y$ 的边 $e$. 设 $x'$ 和 $y'$ 分别是 $H$ 上 $x$ 和 $y$ 的后继. 考虑沿 $H$ 从 $x'$ 到 $y$ 的路 $P$，然后沿 $\{y, x\}$，再从相反的方向沿 $H$ 从 $x$ 到 $y'$. 如果边 $\{x', y'\}$ 属于 $G$，我们就做完了. 否则，用定理 4.3 的证明中的论证说明 $P$ 能通过移去一条边再增加两条边围成一个回路.

更一步的推广见 L. Lovász(1979).

**问题 4G** 证明当 $z_i>0$ 时，$S$ 的最大值仅出现在一个团的点上.

**问题 4H** 对有一个公共顶点的边的对用两种方式计数.

**问题 5A** (i)给定二部图的一部 $A\subseteq X$，对一个端点在 $A$ 中且另一个端点在 $\Gamma(A)$ 中的边计数.

(ii)没有完美匹配的三价图是 4 个顶点 6 条边的图，其中 1 个顶点与 3 条非环边关联，其余 3 个顶点与环边关联. 由适当的简单图代替这些环边.

(iii)提示与(i)的相同.

**问题 5B** 构造大小为 $m_i$ 的集合 $A_i$ 的一个序列，仅当使条件 $H$ 满足所需时才使用一个新元素. 在 Van Lint(1974)的 41 页给出了一个解答.

**问题 5C** 对矩阵的非零项的数目用归纳法. 定理 5.5 的论证可以类似地加以应用.

**问题 5D** 定理 5.5.

**问题 5E** 分别用 1，2 表示 SDR 的数目，把 $A_1$ 按照 $i<n$ 的 $S_i$ 表示. 参见问题 14A.

**问题 5F** 对满足所有的 $k$，$x_k\in A_k$ 且 $x_i=x_j$ 的集合 $\{x_1, x_2, \cdots, x_n\}$ 的数目进行计数.

**问题 5G** (i)是容易的，但(ii)有些棘手. 参考例 10.1.

546

**问题 6A** 利用整数 $a_i$ 的大小和指标定义一个偏序集.

**问题 6B** (i)考虑 $A$ 和 $\overline{A}$. (ii)设 $x$ 在所有的集合中.

**问题 6C** 证明大的集合可以用它们的补代替，并应用定理 6.5.

**问题 6D** (i)这些子集中没有两个在同一链上. (ii)用归纳法.

**问题 6E** 参见 C. Greene and D. Kleitman, Strong versions of Sperner's Theorem, *J. Combinatorial Theory*(A)20(1976), 80-88.

**问题 7A** 这是最大流算法的直接应用. 最小割的容量是 20.

**问题 7B** 给定一个非零强度的流 $f$，证明 $f(e)\neq 0$ 的边 $e$ 包含从 $s$ 到 $t$ 的一条简单有向路. 减去对应初等流的一个标量倍数以得到较 $f$ 在更多的边上为零的流 $f'$，并由归纳法进行.

对所要求的例子，4 个顶点就够了.

**问题 7C** 考虑一个最大流 $f$. 由方程(7.1)，从 $X_i$ 到 $Y_i$ 的边是饱和的，而且从 $Y_i$ 到 $X_i$ 的流值为零.

**问题 7D** 给定顶点为 $X\cup Y$ 的二部图 $G$，通过增加两个顶点 $s$ 和 $t$ 构造一个网络，从 $s$ 指向 $X$ 的元素的边的容量为 1，并且从 $Y$ 的元素指向 $t$ 的边的容量为 1. 所有原始的边从 $X$ 到 $Y$ 定向；对这些边赋予大的容量(比如说 $|X|+1$)是方便的，于是这样的边不出现在最小割中. 解释为什么在 $G$ 中存在一个从 $X$ 到 $Y$ 的完美匹配当且仅当这个网络有最大流强度 $X$.

**问题 7E** (iv)对 $d=2$，应用定理 7.2 于该图的关联矩阵. (这个结果也是定理 1.2 的直接结果.)(v)考虑一个二部图 $G$ 的二部关联矩阵 $M$，其定义如下. 比如说 $G$ 有两部分$(X, Y)$. $M$ 的行由 $X$ 中的顶点指示，且 $M$ 的列由 $Y$ 中的顶点指示. 在 $x(x\in X)$行和 $y(y\in Y)$列的项是连结 $x$ 和 $y$ 的边的数目(若 $G$ 为简单图，$M$ 中的项是 0 或 1). [547]

**问题 7F** 设 $T$ 为 $D$ 的支撑树. 证明对 $D$ 的不在 $T$ 中的 $|E(D)|-|V(D)|+1$ 条边的任意一个实数赋值，存在唯一的一个途径把这一赋值扩展为 $D$ 上的循环流 $f$. 回想树至少有一条边有一个一价顶点是有用的.

**问题 8A** 假定 $n$ 个相继元素的某个子序列出现两次. 证明 $\alpha$ 满足次数小于 $n$ 的一个方程.

**问题 8B** 该有向图的顶点是{0, 1, 2}的有序数对；图的边是 27 个有序三元组.

**问题 8C** 该序列一定包含四个 0 和四个 1. 三个相继的 0 迫使 00010111 不起作用；数对 00 一定出现两次，这迫使 00110011 也不起作用.

**问题 8D** 由于 $G_n$ 中每个顶点的入次为 2 且出次为 2，我们确实得到从 $00\cdots0$ 到 $00\cdots0$ 的一条闭路. 最后一条边一定来自 $10\cdots0$(它与二进制的 1 等同). 这条边被用到这一事实蕴涵从 $1=10\cdots0$ 到 $0\cdots01$ 的边已被用过. 于是，我们到达顶点 1 两次，即从 $2=010\cdots0$ 和从 $3=110\cdots0$各一次. 根据与上面相同的理由，2 和 3 都被进入了两次. 由归纳法，我们看到在穿过 $G_n$ 的路上所有顶点被访问两次，从而证明了论断.

**问题 9A** 应用 Winkler 的算法.

**问题 9B** 如定理 9.2 中一样，易于找到一个长度 $n$ 的平凡的编址. 该图的直径是多少?

**问题 9C** 利用定理 9.1 和定理 9.6. 在计算中会出现$\sum k\cos(kx)$. $\sum k\cos(kx)$是$\sum\sin(kx)$的导数，该和可以通过乘以 $\sin\left(\frac{1}{2}x\right)$求得.

**问题 9D** 参见定理 9.7(4).

**问题 10A** 利用定理 10.1，这里 $E_i(i=1, 2, 3, 4)$分别是$\leqslant 1000$ 且能被 2，3，5，7 整除的整数. [548]

**问题 10B** 利用容斥原理以及如果 $f(i)=0$，则$(x-i)$整除 $f(x)$.

**问题 10C** 利用$\lfloor x\rfloor=\sum_{k\leqslant x}1$ 和定理 10.3.

**问题 10D** $\sum a_n n^{-s}$与$\sum b_m m^{-s}$相乘. 确定 $k^{-s}$的系数，并利用定理 10.3.

**问题 10E** 确定$\sum_{d|n}\log f_d(z)$；利用定理 10.3 或定理 10.4.

**问题 10F** 显然有 $2n+1$ 种染色. 对由 $i$ 红色且 $i-1$ 蓝色的染色构成的一个集合 $E_i$ 应用

容斥原理. 为确定 $N_j$，利用例 10.6.

对直接的解法，计算

$$\sum_{n=0}^{\infty}\sum_{k=0}^{n}(-1)^k\binom{2n-k}{k}2^{2n-2k}x^{2n}.$$

为此，利用(10.6)和$\sum(2n+1)x^{2n}=\left(\frac{x}{1-x^2}\right)'$.

**问题 10G** 利用定理 10.1.

**问题 10H** 对不固定 1，2，…，$n-k$ 中任何一个的 1，2，…，$n$ 的排列计数.

**问题 11A** 考虑规模为 $n\times k$ 的全幺矩阵. 邻接一列 0，然后通过添加类型(0，…，0，1)的行使之成为方阵.

**问题 11B** (i)定理 5.3；(ii)定理 11.5；(iii)利用矩阵 $J_k$ 的直积.

**问题 11C** 确定满足 $a_{ij}=|A_i\cap B_j|$ 的 $A=(a_{ij})$. 为找出这个矩阵的积和式，比较夫妻问题.

**问题 11D** 利用定理 11.7.

549 **问题 11E** 由矩阵第一行和第一列的展开，计算对应的积和式 $B_n$. 证明 $B_n=B_{n-1}+B_{n-2}-2$. 于是$\{B_n-2\mid n\geqslant 3\}$是一个斐波那契序列. 也见问题 5E.

**问题 12A** 利用定理 12.1.

**问题 12B** 假设 $AA^{\mathrm{T}}$ 是可分解的. 通过考虑 $A$ 的某一行、其非零项，以及它与其他行的内积解释 0 项的区组.

**问题 12C** 对行的对以及类似地对列的对作四个平均运算. 注意元素 $a_{55}$ 在这些运算期间不改变. 确定积和式并最小化. 这证明矩阵在开始时是$\frac{1}{5}J$.

**问题 13A** 利用定理 13.1.

**问题 13B** (i)$(1-x)$的两个幂相乘. (ii)设 $k$ 在位置 $a+1$；哪一项能先于这一项？

**问题 13C** (i)选择 $A_1$，然后选择 $A_2$ 作为 $A_1$ 的补集的子集；确定二项式系数之积的和. (ii)考虑一个 $2\times n$ 的矩阵，其行分别是 $A_1$ 和 $A_2$ 的特征函数. 把对 $A_1$ 和 $A_2$ 的条件化成对这个矩阵的条件.

**问题 13D** 首先，固定$\mathcal{A}$中的集合的并 $U$. 应用例 13.6，然后对 $U$ 中所有的选择求和. 答案表明我们原本可以找到一个更好的解. 为找到这个更好的解，再次把$\mathcal{A}$用规模为 $k\times n$ 的(0，1)-矩阵表示. 在这个矩阵上邻接“特殊的”一行，即$\mathcal{A}$的集合的并的特征函数. 计算这些(0，1)-矩阵的数目，其中有一个 1 在“特殊的”行中特定的位置.

**问题 13E** 对每一条路径，考虑类型$(x,y)\to(x+1,y+1)$的最后一步. 利用定理 13.1. 对最后一个问题，在 $n+k$ 个可能的位置插入 $k$ 个球；设 $x_k$ 是第 $k$ 个球前面的间隔长度.

550 **问题 13F** (i)用归纳法证明. 如果 1 到 $n-1$ 的置换写成圈的一个积，有 $n$ 种方式邻接元素 $n$，其中之一多出一个圈. (ii)在定理 13.7 中，两边对 $k$ 求和；利用(13.5).

**问题 13G** 把(13.13)代入(13.11)并改变求和顺序.

**问题 13H** 利用(10.6).

**问题 13I** 利用 123 页[⊖]上的关系 $F(a)=G(a)$.

**问题 13J** 利用 $x=\zeta$ 的二项式公式，这里 $\zeta^3=1$.

**问题 13K** 对一个 $n$-集合分成 $n-2$ 个部分的划分直接计数.

**问题 14A** (i)序列以 10 或 1 结束. 建立斐波那契递推式并尝试 $a_n=t^n$ 作为一个解(利用线性性). 也可以利用例 14.3 中的方法.

(ii)把 $b_n$ 用这些序列中以 1 结束的序列的数目 $c_n$ 表示. 找出 $c_n$ 的一个递推式. 常数 $c$ 是一个四次多项式方程的最大根；它接近 1.220 75.

**问题 14B** 考虑一棵三价种植平面树 $T$. 构造一棵新树 $T'$如下. 取 $T$ 的根和它所有的 3 次顶点作为顶点. 在 $T'$中连结两个顶点，如果在 $T$ 中从一个顶点到另一个顶点的路径恰用了一条向左倾斜的边(见图 14.3). 最后，在底上加入一个新的根. 表明怎样反转这一映射. 证明 $T'$的顶点数等于 $T$ 中 1 次顶点的数目. 参见 J. H. van Lint, *Combinatorial Theory Seminar, Eindhoven University of Technology* 的第 25 页, Lecture Notes in Mathematics 382, Springer-Verlag, 1974.

**问题 14C** 固定一条边；轮流给其他边标号：$a$，$b$，$c$，…. 给弦以明显的名称；小心这些名称的顺序. 也参见 Van Lint(1974)的第 25 页.

**问题 14D** 利用图 2.2 的方法. 一个不动点产生一个树形图；其余的是一个没有不动点的映射. 参见(14.15). 取 $M_1(0)=1$，$A(0)=0$. [551]

**问题 14E** 固定一条边，然后考虑它所属的四边形. 其余的三条边可能把$(n+1)$边形分成空的多边形；见(14.10). 利用定理 14.3 解 $f=x+f^3$.

由不相交的对角线把一个$(n+1)$边形划分成四边形，当 $n$ 为偶数分法数是 0，且当 $n=2k+1$ 时分法数是$\frac{1}{3k+1}\binom{3k+1}{k}$，其组合证明如下. 因为 $n$ 是偶数的情形是平凡的，我们假设 $n=2k+1$. 在剖分中有 $k-1$ 条对角线和 $k$ 个四边形. 在每个四边形及它的每条边上放一个顶点；固定一个边上的顶点作为根. 四边形的顶点被一条边连结，如果四边形共享一条对角线；边上的顶点与它所在的四边形中的顶点有边相连. 环绕刚定义的树画一条步路，由符号 $x$ 和 $y$ 的序列表示，到达以前不曾访问过的四边形中的顶点用 $x$ 表示，类似地对边上的顶点用 $y$ 表示. 我们找到有 $k$ 个符号 $x$ 和 $2k+1$ 个符号 $y$ 的一个序列. 我们知道，见例 10.6，有$\frac{1}{3k+1}\binom{3k+1}{k}$个这种类型的循环序列. 剩下要证明这些循环序列和描述树的序列之间的一一对应. 描述 $x$，$y$ 序列如下：一个 $x$ 对应 $X$-$Y$ 平面上向右一个单位且向上一个单位的一步，一个 $y$ 对应向右一个单位的一步和向下 $k/(2k+1)$步. 这条步路从$(0, 0)$开始且在$(3k+1, 0)$结束，中间不与 $X$ 轴相交. 如果按照相同的方式描述给定类型的一个循环序列，它会有一个唯一的最小值，因为$(k, 2k+1)=1$. 这将给出唯一的起始点使它与树中的一棵对应.

**问题 14F** 见附录 2 中的形式运算. 取对数然后用定理 10.3.

**问题 14G** 证明与例 14.11 的等价性.

---

⊖ 这是指原书页码，与书中页边标注的页码一致. ——编辑注

**问题 14H** 如例 14.8 中那样构造一条步路并找一个最低点.

**问题 14I** (i)见(14.10). (ii)把一个顶点放在该圆上，比如说放在 1 和 $2n$ 之间. 这将是一棵树的根. 在每个区域放一个顶点并按照明显的方式连结顶点. 证明与一个卡塔兰问题的等

552 价性. 见 Van Lint(1974)的第 26 页.

**问题 14J** 一个标号的二价正则图是(标号的)多边形的并. 应用定理 14.2.

**问题 14K** 称步路的数目为 $A_{4n}$ 并定义 $A(z):=1+\sum_{n=1}^{\infty}A_{4n}z^{4n}$. 如果 $B_{2n}$ 是从 $(0,0)$ 到 $(n,n)$ 且避开点 $(i,i)$ 的步路数,则从(14.12)可以知道 $B(z):=\sum_{n=1}^{\infty}B_{2n}z^{2n}=1-\sqrt{1-4z^2}$. 通过考虑每条步路第一次与 $x=y$ 的交叉寻找 $A(z)$ 和 $B(z)$ 之间的关系.

通过寻找 $A_{4n}$ 计数的步路与例 14.8 中计数的步路之间的一个一一映射，也可以证明这个结果. 这并非易事. 解答参见 W. Nichols 在 *American Mathematical Monthly* 94(1987)上对问题 3096 的解.

**问题 14L** 证明 $a_n=3a_{n-1}-a_{n-2}$，以及 $F_{2n}$ 满足同样的递推关系.

**问题 14M** 因为 $g$ 有 $k$ 个不动点，计算它们的数目及合适的 $f$ 的数目并在 $k$ 上求和；对于象的规模为 $i$ 的 $f$，分裂$\{1, 2, \cdots, r\}$为原象，对 $f$ 及合适的 $g$ 的数目计数，在 $i$ 上求和. 利用(13.9)和(13.11). 这是 *American Mathematical Monthly* 94(1988)中对问题 3057 的解答，由 J. M. Freeman、S. C. Locke 和 H. Niederhausen 给出.

**问题 14N** 引入 $b_{k,n}:=$从$(0, 0)$到$(n, n)$与 $x=y$ 在$(k, k)$两次相交的步路数.

**问题 15A** 在 $x_k=1$ 和 $x_k>1$ 之间进行区分，对 $x_k>1$ 的情形取 $y_i=x_i-1$. 用归纳法.

**问题 15B** 设 $E$，$I$ 和 $S$ 分别表示等边三角形、等腰三角形和不等边三角形的数目. 计算 $E$，$I+E$，并用 $E$，$I$ 和 $S$ 表示$\binom{n}{3}$.

(这个证明属于 J. S. Frame，*American Mathematical Monthly* 47(1940)，664.)

**问题 15C** 用部分分式. 用$(1-x)^{-t}$的系数和(10.6)求 $c$.

**问题 15D** 对 $n$ 分成 $k$ 部分且 3 在位置 $j$ 的分解进行计数，对所有的 $j$ 这样做并求和(因此

553 有 $m$ 个部分是 3 的分解被数了 $m$ 次).

有一个更普遍结果的第二个解法如下.首先证明在所有可能分解的列表中恰好有$(n+1)\cdot 2^{n-2}$个整数.这可通过利用红球的论证完成.然后通过对 $n$ 进行归纳证明,当 $1\leqslant m<n$ 时,$n$ 的 $2^{n-1}$ 个分解的列表中恰包含$(n-m+3)2^{n-m-2}$次整数 $m$. 为此,应用公式 $1+\sum_{k=1}^{n-1}(k+3)2^{k-2}=(n+1)\cdot 2^{n-2}$,该式也由归纳法证明.

**问题 15E** 不考虑第一列.

**问题 15F** 对不相等的奇数部分，用“钩”状的图形构成 Ferrers 图并按通常的方式阅读该图.

**问题 15G** 证明与例 14.8 的一个对应.

**问题 15H** 见第 13 章.

**问题 15I** 推广定理 15.4.

**问题 15J** 应用定理 15.10 于一个 $n \times n$ 正方形.

**问题 16A** 用归纳法，比较 $\boldsymbol{r}$ 和 $\boldsymbol{s}$ 的初始片断.

**问题 16B** 确定行和为 $\boldsymbol{r}$ 且列和为 $\boldsymbol{r}^*$ 的一个矩阵的第一列. 用归纳法.

**问题 16C** 应用问题 16A 并转换边. 另一种可能性是由图的邻接矩阵描述该图，所用思路与定理 16.2 的证明中所用的相同.

**问题 16D** 仅利用每个 $s_i$ 至多是 $n$ 的事实估计 $s_1+\cdots+s_n=\frac{1}{2}n^2$ 的解的数目.

**问题 16E** 对"当"这一部分，首先注意到存在一个次序列为 $(n-1, \cdots, 2, 1, 0)$ 的竞赛图. 然后利用问题 16A. 证明如果在一个竞赛图中，$x$ 的出次大于 $y$ 的出次，则在相同的顶点集上有一个竞赛图，它有相同的出次，但 $x$ 的出次比原图小 1、$y$ 的入次比原图大 1 除外. 通过至多改变两条边的方向可以做到这一点.

**问题 16F** 对推广，考虑由选择按字典序的 $k$-子集合的前 $m$ 个给出的超图. 对"当"这一部分，再次利用问题 16A. 554

**问题 16G** $A(5, 3)=A(5, 2)$. 见(16.2). 直接计数是可能的：(i)固定第一行为(1，1，0，0，0)，这意味着最终的结果一定要乘以 10. (ii)在位置(2，1)置一个 1，这意味着最终结果也应乘以 4. (iii)分成两种情形：1 在位置(2，2)，等等；或 1 在位置(2，3)，在这种情形引入一个因子 3，等等.

另一个解通过观察到 $\mathcal{A}^*(5, 2)$ 的基数为 $\frac{1}{2}5!\,4!=1440$ 而得到，而且在 $\mathcal{A}(5, 2)$ 中有 $\left(\binom{5}{2}\right)^2 \cdot 3!=600$ 个可分解的矩阵.

**问题 16H** 在情形 1，有 $n-1$ 种可能的选择. 在情形 2，移去第 1 行和第 1 列，替换 $\mathcal{A}(n-1, 2)$ 中的一个元素，然后以两种方式产生 $\mathcal{A}(n, 2)$ 的一个元素.

**问题 16I** 直接替换.

**问题 17A** 由 $x$ 和 $y$ 指示前两行，$u$ 和 $v$ 指示前两列，在所有这些假设之下我们有 5 阶群的乘法表. 证明 $(v^{-1}u)^2=1$.

**问题 17B** 尽管拉丁方的规模较小，但这已经够困难了！取 $a=1$. 注意这个 1 在左上角的子方阵的类型是 $\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}$，$i=2, 3, 4, 5$. 考虑有这种性质的任意一个拉丁方. 如果(2，3)项不是 4，则改变第 4 行和第 5 行、第 4 列和第 5 列，以及符号 4 和符号 5 的顺序，把这个方阵变成与 4 在位置(2，3)的等价方阵. 此时，只有一种方式完成这个拉丁方. 因此，如果一个拉丁方有任何一个单元有诸如左上角为 1 的性质，则它等价于这个拉丁方.

利用同类的论证可以证明仅有几种可能的不等价的 5 阶拉丁方. 对一些拉丁方，必须建立等价性，这是一件冗长乏味的工作.

**问题 17C** 对这个问题，建议反复实验. 参见第 22 章.

**问题 17D** 充分性由一个例子证明(可以但并非一定要用定理 17.1). 对必要性，注意到附 555

加新的一列于一个 $m$ 阶的拉丁方需要 $m$ 个新符号.

**问题 17E** 利用定理 17.5 中的算法.

**问题 17F** 对(i),描述一个算法,它从反对角线为常数的已构造的 $n+1$ 阶拉丁方恢复出原始的 $n$ 阶拉丁方. 对(ii),解释为何 $n$ 在反对角线上的 $n$ 阶拉丁方的数目是 $N(n)/n!$.

**问题 17G** (a)对 $n=6$,一个例子是 6,1,5,2,4,3. (b)把差加起来. (c)假定两对相等并求解.

**问题 17H** 以 $n+1$ 替换较小的拉丁方的对角线上的项开始.

**问题 17I** 见例 10.6.

**问题 17J** (i)利用容斥原理. 如果 $k$ 个整数在错误的位置,把 $k$ 写成 $k=2i+j$,这里有 $i$ 对在错误的位置,等等.

(ii)利用规模为 $n$ 的 $J-I$.

**问题 18A** 直接证明,理由与定理 18.1 中关于前三行的理由相同. 证明没有其他行能以三个+开始. 因此,5,6 和 7 行都以++-开始. (为什么?)之后这些行能以唯一的方式被补足. 另一种解法见问题 19D.

**问题 18B** 利用定理 18.1 的方法. 注意行和列的保持 0-对角线的一个排列,对我们使得矩阵成为对称的或反对称的没有帮助. 因此,只有乘以 $-1$ 才可以. 正规化第一行并使第一列(第 0 项除外)全是 1 或全是 $-1$. 现在只需证明项(2,3)和项(3,2)当 $n\equiv 2 \pmod 4$时相等,当 $n\equiv 0 \pmod 4$时相反.

**问题 18C** 一个平凡的练习!

556 **问题 18D** 我们有 $28=1+9+9+9$ 及 $28=1+1+1+25$. 利用前一个. 注意每个 $W_i$ 在对角线上都是 1,且如果有 $w_{ij}=2$,则 $w_{7-i,j}$也是 2;对 $-2$,情况类似. 注意 $U^i$ 在矩阵 $W_j$ 中的出现完全限制了四个矩阵 $W_i$ 的选择. 这些矩阵被证明是有效的.

**问题 18E** 由归纳法证明 $M_n^{(i)}\cdots M_n^{(m)}=\boldsymbol{H}_{2^{m-i+1}}\otimes I_{2^{i-1}}$. 对第二部分,对 $M_n^{(i)}$ 的非零元素进行计数. 见参考文献 E. C. Posner(1968).

**问题 18F** 对两个问题都用归纳法.

**问题 18G** 对(2),证明第一个坐标为 0(或 1)的列的数目至多为 $n$.

**问题 18H** 直接做,见定理 18.4.

**问题 18I** 复习 $Q$ 的性质.

**问题 19A** 对(i)中的同构:用$\mathbb{F}_2^4$中的 0000,1000,0100,0010,0001,1111 给 $K_6$ 的顶点标号,图的边以其端点的标号在$\mathbb{F}_2^4$中的和标号. 这给出 $K_6$ 的边和$\mathbb{F}_2^4$中的 15 个非零向量之间的一个一一对应.

对(ii),考虑三条边(有四种类型)的构形. 这个构造属于 E. S. Kramer(1990),*Discrete Math*. 81,223-224.

**问题 19B** 计算 $b_i$,$i=3,2,1,0$;$b_1\notin\mathbb{Z}$.

**问题 19C** 这是定理 19.4.

**问题 19D** (i)设 $N$ 有列和 $c_i$,则$\sum c_i=66$. 行的所有内积的和是$\sum\binom{c_i}{2}$,用柯西-施瓦茨

不等式．得出所有的列和是 6 且所有的内积是 3 的结论．(ii)为证明唯一性，考虑其补：一个 2-(11，5，2)设计．不失一般性，第 1 行是(11111000000)，其余的 10 行以$\binom{5}{2}$个对(110…)，(1010…)，等等开始，然后证明从第 2 行到第 5 行可以用一种方式完成．还剩下 6×6 方阵要完成．初看起来，似乎有两种方式可以做到这一点．寻找把一个映入另一个的一个置换． 557

**问题 19E** 用 $a_i$ 表示与 $B$ 交于 $i$ 个点的区组的数目．计算 $\sum a_i$，$\sum ia_i$ 及 $\sum\binom{i}{2}a_i$．利用形式 $\sum(i-c)^2a_i$ 导出 $a_0$ 的一个不等式．与定理 19.9 比较．

**问题 19F** 映射 $x\mapsto 2x$ 有 6 条轨道，其中两条太长而不能用(例如(1，2，4，8，16，11))．见例 28.2.

**问题 19G** 利用对应的正交阵列．利用通常的{0，1}到{1，-1}的映射．

**问题 19H** 对(1)用(19.2)或(19.4)．对(3)计算对子 $p$，$q\notin B$ 的数目，它们包含在交于 $p$ 的区组中．由此找到$\mathcal{D}^B$ 的参数．对(4)，首先假设$\mathcal{D}^B$ 是一个单一的区组．考虑例 19.3．在其他情形费希尔不等式给出 $k\geqslant(\lambda+1)(\lambda+2)$．现在，把 $b_0$ 表示为 $k$ 和 $\lambda$ 的分数并导出 $k$ 一定整除 $2(\lambda+1)(\lambda+2)$．

**问题 19I** (i)固定 $O$ 上的一点 $x$．计算对子$(y, L)$的数目，$y\in O$，$L$ 是经过 $x$ 和 $y$ 的一条线．(ii)由(i)看到，如果 $|O|=n+2$，则每条交于 $O$ 的线与它相交两次．取一个点 $z\notin O$ 并对过 $z$ 与 $O$ 相交的线进行计数．(iii)取任意 4 个点，没有 3 点在一条线上．这些点确定 6 条线，这些线一起包含平面的 19 个点．

**问题 19J** 对 $p_1$ 到 $p_5$ 取(1，0，0)，(0，1，0)，(0，0，1)，(1，1，1)和$(1, t, t^2)$，证明为产生 $p_6=(1, x, x^2)$有两种方式给这些点分组，这里 $x=t/(1+t)$．

**问题 19K** 设 $B_1\sim B_2$．与 $B_1$ 相交的区组有多少？取 $x\in B_1$，$y\in B_2$，与 $B_1$ 和 $B_2$ 都相交的区组有多少？有 $n+1$ 个等价类，每个等价类带有 $n$ 条线(区组)．对每个类附加一个点，这个点作为一个额外的点附加到这个类的每条线上，等等．

**问题 19L** 利用定理 19.11．考虑模 3 的方程．

**问题 19M** 对偶数 $v$，用二次型，如定理 19.11 的证明中那样．见 J. H. van Lint and J. J. Seidel(1966)，Equilateral point sets in elliptic geometry，*Proc. Kon. Nederl. Akad. Wetensch.* 69，335-348. 558

**问题 19N** (a)如果 $|V|=1$，例 19.14 中的方法仍然有效$(85=7(13-1)+1)$．(b)$15=7(3-1)+1$．

**问题 19O** 考虑 $n\times b$ 关联矩阵 $N$，这里 $b=|\mathcal{A}|$．在情形(i)，检验 $N^\top N$ 模 2 非奇异．对(ii)，设 $N_1$ 是由 $N$ 附加全幺的一列得到的，并证明 $N_1^\top N_1$ 的秩至少为 $b$ 模 2.

**问题 19P** 所显示的和中最后一个应等于 0．这蕴涵 $\mu_i$ 等于 1 或 2.

**问题 19Q** 用归纳法，从 $t=2$ 开始归纳．用两种方式对有序三元组$(x, A, B)$进行计数，这里 $A$ 和 $B$ 是不同的区组，两者都包含点 $x$．

**问题 19R** 如例 19.6 中那样表示线，并利用这是一个循环表示这一事实．由用在 SDR 中

“第一个”元素的数目区分不同的情形.

**问题 19S** 用对 $k$ 进行归纳给出一个构造是可能的，但用$\mathbb{F}_2^k$作为点集给出一个直接的构造更为迅速. 复习例 19.1.

**问题 19T** 利用问题 19H 的结果. 扩展出现在第 20 章.

**问题 19U** 利用定理 5.5.

**问题 20A** 利用(20.5).

**问题 20B** 对字的最后两个比特用鸽巢原理. 一个有三个字的二元码容易处理!

**问题 20C** 对这种违反码字条件的三种方式中的每一种，改变一个适当的坐标补救这种局面.

**问题 20D** (i)生成矩阵的行对应$\pm \boldsymbol{a}_i$，$i=1$，…，$n$，这里 $\boldsymbol{a}_i$ 是阿达马矩阵的行. 设 $\boldsymbol{u}\in\mathbb{F}_2^n$，这里 $n=2^{2k}$. 我们用 $\boldsymbol{u}^\star$ 记$\pm1$表示. 计算$\sum\langle \boldsymbol{u}^\star, \boldsymbol{a}_i\rangle^2$ 以找出上界.

(ii)对相等性，首先寻找 $\boldsymbol{z}$ 的重量. 然后用码字对应线性函数这一事实，再对 $\boldsymbol{x}$ 附加一个线性函数，产生一个等价的二次型.

[559]

**问题 20E** (i)见问题 20A. (ii)对由重量为 7 的码字“覆盖”的重量为 5 的码字进行计数. 利用这个想法，对 $A_i$ 建立线性方程组.

**问题 20F** 离重量为 $e+1$ 的一个字的距离$\leqslant e$ 的码字一定有重量 $2e+1$.

**问题 20G** 在长度为 $2^r-1$ 的二元汉明码的对偶中，码字可以等同于$\mathbb{F}_2^r$上的线性泛函(参见第 18 章中里德-米勒码的几何描述)；每个非零码字有重量 $2^{r-1}$.

**问题 20H** 利用(19.6)及 $G_{24}$是线性的且有最小的重量 8 这个事实；注意线对有$\binom{21}{2}$个. 如果 $\alpha=1$，考虑平面上 7-点的构形 $B^*$. 任意与 $B^*$ 相交的线一定与它交于 1 个点或 3 个点. 有多少条线与 $B^*$ 交于 3 个点?

**问题 20I** (i)找出 $C$ 的标准生成矩阵. (ii)条件(1)和(2)显然定义一个线性码. 在(1)中对奇偶性有两种选择；在(2)中对码字有 $4^3$ 种选择；在 $A$ 的五列中此时有两种可能性. (不在最后一个中!)对选择到“偶”，显然 $C$ 中的一个非零码字迫使重量$\geqslant 8$；**0** 必须单独处理. 对选择到“奇”，显然我们得到至少为 6 的一个重量；条件(1)保证等号不能成立. 有关戈莱码的这一出色描述的更多内容及许多结论，见 J. H. Conway and N. J. A. Sloane，*Sphere Packings, Lattices and Groups* 的第 11 章，Springer-Verlag，1988.

**问题 20J** 自对偶如例 20.6 中那样处理. 在 $Sym_{12}$中所有的重量都能被 3 整除. 考虑生成矩阵中两行的线性组合，然后得出结合另一行时会发生什么的结论. 利用(20.5).

**问题 20K** 由对 $r$ 的归纳法证明这一推广. 对每个 $r$，找到其列没有一个是常数向量的矩阵. 对归纳步骤，$r-1$ 行的矩阵分别添加全 0，全 1 和全 2 的一行，把这三个有 $r$ 行的矩阵连接起来，然后添加三个适当的列.

[560]

**问题 20L** 本章的提示就够了.

**问题 21A** 论证与用于(21.4)的相同，现在处理的是不等式.

**问题 21B** 利用整数条件. 也见第 4 章的参考文献 A. J. Hoffman and R. R. Singleton (1960).

**问题 21C** 利用(19.2)，见问题 20F. 如果两个区组不相交，对与这两个区组中的每一个

交于两个点的区组进行计数．仅与它们之中的一个相交的区组有多少？对 $\mu=6$ 的证明，用类似的计数论证．（区分为几种情形！）

**问题 21D** 假设这样一个图存在．取一个顶点 $x$ 并考虑集合 $\Gamma(x)$ 和 $\Delta(x)$．我们把它们作为一个设计的点和区组考虑．证明这是一个 2-(9，4，3)设计．其次，固定这个设计的一个区组，设 $a_i$ 为与这个区组交于 $i$ 个点的区组的数目．证明 $a_0\leqslant 1$（见问题 19E），并证明 $\Delta(x)$ 有 5 度的点蕴涵 $a_0$ 至少为 5.

**问题 21E** 直接做前两个问题．对第三个问题，参照矩阵论的教科书或第 31 章．我们暗指的定理说一个对称矩阵 $A$ 的主子矩阵 $B$ 的特征值受矩阵 $A$ 的最大特征值和最小特征值所限制．为证明这一点，考虑任意一个向量 $\mathbf{x}$ 并计算 $\mathbf{x}^\top A\mathbf{x}/\mathbf{x}^\top\mathbf{x}$．限定 $\mathbf{x}$ 为 0 附在后面的 $B$ 的特征向量.

**问题 21F** 复习定理 21.5 的证明．证明 $\Gamma(x)=\overline{K_{n-1,n-1}}$．定义大团是一个规模为 $n$ 的团，并证明任意一条边恰好在一个大团上．证明恰有 $2n$ 个大团，它们落在 $n$ 的两个类中，使得落入同一类的大团是不相交的．见 S. S. Shrikhande，The uniqueness of the $L_2$ association scheme，*Ann. Math. Stat.* 30(1959)，781-798.

**问题 21G** 对旗标和其他构形进行计数，例如，交叉的两条线和它们之一中的一个点． 561

**问题 21H** 对 $v$，见问题 21E；$k$ 是显然的．取线 $L$ 上的两个点．与这两个点都相连的点在 $L$ 上或者在一条线上，这是通过它们之中一个点的 $R-1$ 条线之一．类似的论证得出 $\mu$．对 $r$ 和 $s$ 见(21.6).

**问题 21I** 在 $\Gamma(x)$ 上用 $\mu=1$ 这一事实．然后考虑 $\{x\}\cup\Gamma(x)$.

**问题 21J** 等式(21.8)导致类似(21.6)的一个等式，但用 $t$ 代替 $k$．尽管 $A$ 不是对称的，特征值 $\neq k$ 的特征向量与 $\mathbf{j}$ 正交.

**问题 21K** 证明：如果 $(\lambda-\mu)^2+4(t-\mu)$ 不是一个平方，则特征值有重数 1，$f$ 和 $g$，这里 $f=g=\frac{1}{2}(v-1)$．然后证明 $A=A^\top=J-I$ 且 $AA^\top=lJ+(l+1)I$，这里 $v=4l+3$．定义 $Q:=A-A^\top$.

**问题 21L** 设 $d:=\sqrt{(\lambda-\mu)^2+4(t-\mu)}$．应用(21.8)于 $\mathbf{j}$，然后证明 $d$ 整除 $(k-1)^2$．利用 $4k-7=d^2$，证明 $d$ 一定整除 9.

对 $v=18$，利用矩阵

$$\begin{bmatrix} cI & (c-1)I+J \\ (\bar{c}-1)I+J & \bar{c}I \end{bmatrix},$$

并由例 21.11 中的矩阵 $C$ 代替 $c$ 且由 $C^2$ 代替 $d$ 以得到一个规模为 $18\times18$ 的矩阵 $A$.

**问题 21M** (i)考虑 $\Gamma(x)\cap\Gamma(y)$，这里 $(xy)$ 是一条边．(ii)证明 $\bar{G}$ 也是邻域正则的.

**问题 21N** (i)$\Gamma(x_1)=C\cup B$ 是 $a$ 度正则的，因此 $|CB|=a|C|-|CC|$，等等.

(ii)从(i)的关系中消去 $|BC|$ 和 $|BD|$.

(iii)交换 $x_1$ 和 $x_2$．利用 $d_1\neq d_2$.

(iv)把 $d_i$ 用 $k_i$，$a$，$\bar{a}$ 及 $G$ 的顶点数 $n$ 表示．然后证明 $k_1+k_2=2n-3\bar{a}-a-5$.

**问题 21O** (i)是直截了当的．例如$\lambda=(n+3)/2$．(ii)如果一个团$C$的 4 个三元组包含一个点$x$，则这个团的所有三元组一定包含$x$．(iii)如果$n>15$，则在一个三元系的图中，规模为$(n-1)/2$的团与这个三元系的点是一一对应的．

562

**问题 21P** 等号成立蕴涵$srg(a^2+a+1, a+1, 1, 1)$的存在性．用定理 21.1．仅$a=1$是可能的且$K_3$显然没有在 4 个顶点上的一个回路．

**问题 21Q** 表示朋友关系的图$G$或者是有一个公共顶点的所有三角形的并，或者$G$是正则的．利用定理 21.1．

**问题 22A** 由计算证明一个$(n, n)$-网的图的补有$(n, 1)$-网的图的参数．然后证明它是一个$(n, 1)$-网的图，即存在点分成规模为$n$的$n$个集合的一个划分，集合中没有两个点是共线的．

(更一般地，一个$(n, r)$-网是$(n, n+1)$-网的补当且仅当$(n, r)$-网的图的补是一个$(n, n+1-r)$-网的图．)

**问题 22B** 利用该问题之前描述的域的构造．例如，取$S(x, y):=(x+y)/2$，$q$为奇数．

对偶数$q$，用$A$和$S$确定网球混合双打的时间表．假设有$q$对配偶——对$i\in\mathbb{F}_q$，$i$先生和$i$女士．设在$S(i, j)$轮，$i$女士和$j$女士与各自的搭档$A(i, j)$和$A(j, i)$彼此交锋．有$q-1$轮，它们由$S$中对角线之外的符号标号，每个人在这些轮中恰好比赛了一局．可以发现在整个锦标赛中没有一个人遇到她或他的配偶作为搭档或对手，但对其他每个人恰有一次作为对手，而且与配偶之外的每个异性恰有一次作为搭档．对奇数$q$，我们有$q$轮，其中的每一轮有一对夫妇袖手旁观．

**问题 22C** 证明$m$，$m+1$，$t$和$u$中的每一个有以下性质：对每个素数$p<x$，它们或者与$p$互素或者能被$p^x$整除．

563

**问题 22D** 复习两两正交的拉丁方的集合和横截设计之间的联系．

**问题 22E** 利用定理 22.6．

**问题 22F** $A$的列由 1 到$k$之间的整数组成．对$A$和$S$的每一列，在$A$的该列中，一个整数$i$由$S$中该列的第$i$个元素替换．通过加上适当的列和一行，完成$OA(v, c+1)$．

**问题 22G** 证明与定理 22.6 的证明类似．现在也需要一个$(\mathcal{V}, \mathcal{K}, \mathcal{D})$和一个$TD(v, k)$．

**问题 22H** 利用问题 22F．

**问题 22I** 利用问题 22G．

**问题 22J** 利用问题 22G．

**问题 23A** 注意边的集合$S$的闭包由所有这样的边组成，即每条边的两个端点都在边集为$S$的$G$的生成子图的同一个连通分支中．

**问题 23B** $AG_r(2)$的线的规模为 2．

**问题 23C** 首先处理两条线的并是整个点集的情形．然后说明怎样建立任意两条线的点之间的一一对应．

**问题 23D** 最难的部分是证明$\mathcal{F}=\{F_1\cup F_2 : F_1\in\mathcal{F}_1, F_2\in\mathcal{F}_2\}$．利用$\overline{F_1\cup F_2}$的秩是$F_1$与$F_2$的秩之和这一事实，证明$\overline{F_1\cup F_2}=F_1\cup F_2$．

对组合几何的连通性及几何格的不可约性的全面讨论，见 H. Crapo and G.-C. Rota (1970).

**问题 23E** 假设 $A\cap F=\varnothing$ 且 $\mathrm{rank}(A)+\mathrm{rank}(F)=\mathrm{rank}(\overline{A\cup F})$. 证明当 $A$ 由 $A':=\overline{A\cup\{x\}}$ 代替时这些等式仍成立，这里 $x$ 是不在 $\overline{A\cup F}$ 中的任何一个点.

**问题 23F** 利用(23.4).

**问题 23G** 可以针对 $PG_2(\mathbb{F})$ 进行，不失一般性，假设 $L_1=[1,0,0]$ 且 $L_2=[0,1,0]$. 则(解释原因)当 $a_2=\langle\alpha_2,0,1\rangle$，$b_2=\langle\beta_2,0,1\rangle$ 且 $c_2=\langle\gamma_2,0,1\rangle$ 时，$a_1=\langle 0,\alpha_1,1\rangle$，$b_1=\langle 0,\beta_1,1\rangle$ 且 $c_1=\langle 0,\gamma_1,1\rangle$.

564

**问题 23H** 见第 13 章.

**问题 23I** 仅仅利用 $\lambda$ 的定义.

**问题 24A** 见第 13 章.

**问题 24B** 一个答案是 $e_i=i(m-k+i)$. 考虑秩为 $k$ 的呈阶梯形的 $k\times(n+m)$ 矩阵. 这些矩阵中有多少个在前 $n$ 列中有 $i$ 个首项 1?

**问题 24C** 检验 $x$ 和 $y$ 包含在子空间 $U$ 的一个陪集中当且仅当 $x-y$ 包含在 $U$ 中.

**问题 24D** 对所有的 $n\times n$ 矩阵进行计数.

**问题 24E** 见定理 6.4.

**问题 25A** 对 $r$ 维空间 $W$ 的一个子空间 $U$，设 $f(U)$ 是 $W$ 交于 $U$ 的 $k$-子空间的数目. 利用(25.5).

**问题 25B** 对一个子空间 $U$，设 $f(U)$ 表示其不变向量的集(恰)是 $U$ 的非奇异映射的数目，且 $h(U)$ 是(至少)固定 $U$ 中向量的非奇异线性映射的数目. 用 $n$，$q$ 和 $U$ 的维数容易给出 $h(U)$ 的公式. 对 $f(\{\mathbf{0}\})$，我们需要一个公式.

**问题 25C** 利用(25.2)，对秩为 1 或 2 的 $x$ 计算 $\mu(0,x)$.

**问题 25D** 仅有 $n-1$ 个划分 $x\neq 0_L$(每个由一个规模为 2 的区组和 $n-2$ 个单元素集组成)，满足 $x\wedge a=0_L$.

**问题 25E** 对 $x<z<y$，把从 $x$ 到 $z$ 长度为 $k$ 的一个链扩展为从 $x$ 到 $y$ 长度为 $k+1$ 的一个链.

**问题 25F** 见定理 25.1(iii). 对从 $V$ 到 $S$ 的单射进行计数，然后改变 $|S|$.

**问题 26A** 不在 $A$ 中的一个点 $x$ 上且与 $A$ 相交的线的数目是常数，即与 $x$ 无关.

**问题 26B** 与弧不相交的任意一条线可用来得到把区组划分为平行类的一个划分，对于该线的每个点有一个平行类.

565

**问题 26C** 例如，通过 $\langle 1,0,0\rangle$ 和 $\langle 0,1,0\rangle$ 的线与通过 $\langle 0,0,1\rangle$ 和 $\langle 1,1,1\rangle$ 的线的交点是 $\langle 1,1,0\rangle$.

**问题 26D** 设 $\mu_i$ 为第 $i$ 条线与 $S$ 的交的基数. 如果某个 $\mu_i\geqslant\sqrt{n}+1$，这个不等式是容易的，因此作相反的假设并考虑 $\sum_i(\mu_i-1)(\mu_i-\sqrt{n}-1)$.

**问题 26E** 无论域的特征是偶数还是奇数，$f$ 都是退化的当且仅当对某个满足 $f(\boldsymbol{x})=0$ 的 $\boldsymbol{x}$ 有 $\boldsymbol{x}(C+C^{\mathrm{T}})=0$. 当 $f$ 退化时，为找到这样一个 $\boldsymbol{x}$，取非奇异矩阵 $A$ 的最后两行使得 $ACA^{\mathrm{T}}$

的最后一行和最后一列都是零，$A$ 存在，因为比如说 $x_n$ 在某个射影等价形式中不出现. 也见 J. W. P. Hirschfeld(1979).

**问题 26F** 当 $q=2$ 和 $n=2m-1$ 时，由定理 26.6，$2m$ 个变量的非退化二次型或者有 $2^{2m-1}-2^{m-1}$个零，或者有 $2^{2m-1}+2^{m-1}$个零，这里我们对零向量进行计数. 因此与这样的型对应的码字(长度为 $2^m$ 的向量)的重量是 $2^{2m-1}+2^{m-1}$或 $2^{2m-1}-2^{m-1}$. 这是因为，作为$\mathbb{F}_2$上的函数$x_i^2=x_i$，可以把多项式 $f(\mathbf{x})+a(\mathbf{x})$想象成二次型，或者当有一个常数项 1 时，把它们的补想象成二次型. 证明所有这些型都是非退化的.

另外，还可以证明存在一个"可逆的仿射替换"(例如，这里的 $x_i$ 由 $x_i+1$ 替换)把作为$\mathbb{F}_2^{2m}$上的函数 $f(\mathbf{x})+a(\mathbf{x})$变成 $f(\mathbf{x})$或 $f(\mathbf{x})+1$.

**问题 26G** 证明 $Q'$是 $W$ 中的一个非退化二次曲面是相对直接的. 如果 $n$ 是奇数，证明显而易见. 当 $n$ 是偶数时，可利用定理 26.5 完成证明. 易见如果 $Q'$是双曲的，则 $Q$ 也是双曲的. 然后用(26.4)证明在 $PG_{n-1}(q)$中双曲二次曲面 $Q$ 上的每一个点 $p$ 包含在射影维数为 $n/2-1$的一个平坦面 $F$ 中，$F\subseteq Q$. 验证这样的平坦面包含在 $T_p$ 中，使得平坦面 $F\cap W\subseteq Q'$的维数比 $F$ 的维数少 1.

**问题 26H** 如果点 $x$ 不在线 $\ell$ 上，考虑由 $x$ 和 $\ell$ 确定的面.

566 **问题 26I** 一个三角形的点在一条线上. (iii)见第 21 章.

**问题 26J** 参见射影平面中对弧的论证.

**问题 26K** 考虑三个点. 设 $x_i$ 为补设计中包含这些点中 $i$ 个点的区组的数目. 利用通常的计数论证证明 $x_0+x_3=\lambda$.

**问题 27A** 不难看出偶数号的项彼此等价，类似地奇数号的项彼此等价. 例如，为证明(3)和(4)是等价的，引入一个关联矩阵 $N$，证明一个等价于矩阵等式 $NN^{\top}=(k-\lambda)I+\lambda J$，另一个等价于 $N^{\top}N=(k-\lambda)I+\lambda J$.

**问题 27B** 把$(\mathbb{Z}_2)^4$ 视为域$\mathbb{F}_2$上的一个向量空间. 我们可以假设差集包括零向量. 它生成$(\mathbb{Z}_2)^4$ 且因此包含一组基.

**问题 27C** 分别对 $G\times H$ 中的一个非零元写成 $A\times(H\setminus B)$中的两个元素的差的次数，$(G\setminus A)\times B$ 中的两个元素的差的次数，以及 $A\times(H\setminus B)$中的一个元素与$(G\setminus A)\times B$ 中的一个元素的差的次数进行计数.

**问题 27D** 元素之和乘以任何一个平方，我们想要证明这个和等于 0.

**问题 27E** 我们已说过这个问题类似于定理 27.6 中对 $\lambda_2$ 的计算.

**问题 27F** 利用定理 27.5.(在 L. D. Baumert，*Cyclic Difference Sets*，Lecture Notes in Math. 182，Spring-Verlag，1971 中可以找到一张差集表.)

**问题 27G** 多项式 $y^3+3y+2$(系数在$\mathbb{F}_7$中)的一个零点 $\omega$ 是$\mathbb{F}_{7^3}$的一个本原元.

**问题 27H** $D$ 的平移 $D+g$ 与集合$-D$ 的交的基数是 $g$ 在 $D$ 中作为一个和出现的次数.

567 **问题 27I** 对不同的 $i$ 和 $j$，$\mathbf{x}\in U_i$，$\mathbf{y}\in U_j$，差 $\mathbf{x}-\mathbf{y}$ 组成 $V$ 的所有向量，每个恰出现一次.

**问题 28A** $\mathbb{F}_{p^{t(n+1)}}$的弗罗贝尼乌斯自同构是$\mathbb{F}_{p^{t(n+1)}}$在$\mathbb{F}_{p^t}$上的 1 维和 $n$ 维子空间的对称设计的自同构.

**问题 28B** 可以如引理 28.4 中那样取 $S(x)$，$D=\{1, 2, 4\}$，但这里 $\alpha$ 不是乘子.

**问题 28C** 比如说 $n\equiv 0(\mathrm{mod}\ 10)$，则对任意一个 $x\in D$，$\{x, 2x, 4x, 5x\}\subseteq D$，可以看出差 $x$ 出现两次，除非 $3x=0$. 如果对所有的 $x\in D$，$3x=0$，则对群中的所有 $x$，$3x=0$，$n^2+n+1$ 一定是 3 的一个幂. 证明 $n^2+n+1$ 不能被 9 整除.

**问题 28D** 有这些参数的正规化差集的数目分别为：2，2，4，2，0，4.

**问题 28E** 有两个正规化(15，7，3)差集，它们是等价的，因为一个由另一个的负元构成. 对任何其他的参数不存在规范化差集. 为了在每一种情形证明这一点，首先根据定理 28.7 寻找一个乘子.

例如，对$(v, k, \lambda)=(25, 9, 3)$，例 28.3 证明 2 是假想的正规化差集 $D$ 的一个乘子. 如果群是循环的，则 $D$ 是$\mathbb{Z}_{25}$上 $x\mapsto 2x$ 的圈的并，它们是

$$\{0\},\{5,10,20,15\} \text{ 和 } \mathbb{Z}_{25}\setminus\{0,5,10,15,20\};$$

但没有这样一个并有九个元素. 如果群是基本交换群(指数为 5)，则 $D$ 一定包含 0 和形式为$\{x, 2x, 4x, 8x=3x\}$的两个圈，但差 $x$ 在 0 和这样的一个圈的元素之间已出现 5 次.

**问题 28F** 假设 $D(x^{-1})=D(x)$并利用 $p=2$ 时的引理 28.2.

**问题 28G** 回忆问题 19G 中以这些参数从一个 6 阶的拉丁方中构造一个对称设计.

**问题 28H** 假设 $D(x^q)=D(x)$. 注意 $q^3\equiv -1(\mathrm{mod}\ |H|)$. 证明 $D(x^\alpha)\equiv 0(\mathrm{mod}\ q, H)$并得出 $D(x^\alpha)$的一个系数是 $q+1$，其余的系数都是 1.

568

**问题 28I** 第一部分类似于问题 28H. 然后在 $PG_3(q)$中证明，如果一条线交规模为 $q^2+1$ 的一个集合于 $k\geq 3$ 个点，则这条线上的 $q+1$ 个平面之一包含 $S$ 的多于 $q+1$ 个点.

**问题 29A** 复习定理 20.6 的证明.

**问题 29B** 复习命题 29.5 的证明的后面部分.

**问题 29C** 答案是$(v, k, \lambda)=(4n-1, 2n-1, n-1)$或$(4n-1, 2n, n)$，即阿达马差集或阿达马差集的补. 复习定理 29.7 的证明.

**问题 30A** $A_1A_2=8A_1+8A_2+9A_3$ 且 $A_1^3=90A_0+83A_1+56A_2+36A_3$.

**问题 30B** 由(30.3)，$A_iA_j=\sum_{\alpha=0}^{k}P_i(\alpha)P_j(\alpha)E_\alpha$. 则由(30.4)，

$$NA_iA_j=\sum_{\alpha=0}^{k}P_i(\alpha)P_j(\alpha)\sum_{\beta=0}^{k}Q_\alpha(\beta)A_\beta,$$

显然 $P_{ij}^{\ell}=\frac{1}{N}\sum_{\alpha=0}^{k}P_i(\alpha)P_j(\alpha)Q_\alpha(\ell)$. 第二个特征矩阵 $Q$ 可以通过计算 $P$ 的逆得到(也见定理 30.2).

**问题 30C** 对这个拉丁方图，

$$P=\begin{bmatrix}1 & (n-1)r & (n-1)(n-r+1)\\ 1 & n-r & -n+r-1\\ 1 & -r & r-1\end{bmatrix}.$$

**问题 30D** 为计算 $P$ 的最上一行的项 $P_\ell(0)$，取(30.3)的两端与 $E_0$ 的内积(如定理 30.2 的证明中引入的).

**问题 30E** 这是问题 30B 的对偶.

**问题 30F** 尝试 $|A|=|B|=3$.

**问题 30G** 注意对任意一个自同构 $\sigma$，$|A\cap\sigma(B)|\leqslant 1$. 计算 $G$ 的自同构的数目.

569 **问题 30H** 给定一个来自距离正则图 $G$ 的度量方案，首先注意 $A_1^i$ 是 $A_0$，$A_1$，…，$A_i$ 的线性组合，这里 $A_i$ 的系数是正的. 给定一个 $P$-多项式方案，通过声明 $x$ 和 $y$ 在 $G$ 中是相邻的，当且仅当它们在该方案中是第 1 次结合定义一个图 $G$，并证明两个点是第 $i$ 次结合当且仅当它们在 $G$ 中的距离是 $i$.

**问题 30I** 首先对重量为 8 的字应用问题 20K 中的计数论证，然后寻找满足该条件的其他字. 利用 $j$ 固定的子码和问题 20K 中的码.

**问题 30J** 如果这样的码存在，它将等价于一个码，该码的生成矩阵的第一行是(1111100…0)，下面是$(AB)$，这里 $B$ 生成长度为 8、维数为 5、最小距离至少为 3 的一个码. 现在用[7，4，3]汉明码是唯一的(到等价)这一事实.

**问题 30K** (i)距离只与交的规模有关，只用计数；(ii)该图的度为 4 且两个三元组与交于一个点的费诺平面对应.

**问题 30L** 对 $J(k,v)$，证明一个必要条件是 $1+k(v-k)$ 整除 $\binom{v}{k}$.

**问题 31A** 考虑与特征值 1 对应的 $A_1$ 和 $A_2$ 的特征空间的交.

**问题 31B** 因为邻接矩阵为 $A$ 的一个图 $G$ 的补的邻接矩阵是 $J-I-A$，所以从 $G$ 的特征值容易确定 $\overline{G}$ 的特征值. 第 21 章的前几个例子是等号能成立的例子.

**问题 31C** (i)彼得森图有 3-爪，即由与一个顶点关联的三条边(且没有其他边)构成的四个顶点上的诱导子图. 解释为何一个线图不能包含 3-爪. (ii)矩阵 $N^{\top}N$ 是半正定的且等于 $2I+A$,这里 $A$ 是邻接矩阵.

**问题 31D** $\boldsymbol{x}$ 是全幺时，由等式(31.1)得出一个图的最大特征值的下界由图的最小度界定. 由引理 31.5，$G$ 的最大特征值的下界由 $G$ 的任何一个诱导子图 $H$ 的最小度界定. 如果 570 $\chi(H)=\chi(G)$ 且删去 $H$ 中的任何一个点 $x$ 减小图的色数，则 $\deg(x)\geqslant\chi(H)-1$.

**问题 31E** 如果在邻接矩阵为 $A$ 的一个有向图 $G$ 中，从 $x$ 到 $y$ 不存在有向路，设 $S$ 为顶点 $z$ 的集合，$z$ 使得 $G$ 中不存在从 $x$ 到 $z$ 的一条有向路. 则只要 $a\in S$ 且 $b\in V(G)\setminus S$ 就有 $A(x,y)=0$,因此 $A$ 不是不可约的. 其逆更为容易.

**问题 31F** (i)由直接计算证明 $\boldsymbol{u}_jA=\lambda_j\boldsymbol{u}_j$，这里 $\boldsymbol{\mu}_j=(1,\omega^j,\omega^{2j},\cdots,\omega^{(n-1)j})$. 对(ii)，关于每个特征 $\chi$，定义其坐标由 $G$ 指示的一个向量 $\boldsymbol{u}_\chi$，这里 $\boldsymbol{u}_\chi(g)=\chi(g)$，并证明 $\boldsymbol{u}_\chi A=\lambda_\chi\boldsymbol{u}_\chi$.

**问题 31G** 为证明该引理，证明如果 $\boldsymbol{x}$ 是使得 $\boldsymbol{x}S=\boldsymbol{0}$ 的一个行向量，则 $\boldsymbol{x}\boldsymbol{a}=0$. 应用这个引理于 $S=A+I$，这里 $A$ 是图 $G$ 的邻接矩阵. 这个引理可在 B. Bagchi and N. S. Narasimha Sastry, Even order inversive planes, generalized quadrangles and codes, *Geometriae Dedicata* 22(1987), 137-147 中找到. 这个图问题(由词语"熟人"表述)出自 *American Mathematical Monthly* 108 中的问题 10851，由 D. Beckworth 提出.

**问题 31H** 大部分工作已在定理 31.10 的证明中完成：如果 $G$ 的不同特征值是其度 $d$ 和 $\mu_i$，$i=1,2$，则$(A-\mu_1 I)(A-\mu_2 I)=\frac{1}{v}(d-\mu_1)(d-\mu_2)J$，这里 $A$ 是 $G$ 的邻接矩阵. 这意味

着 $A^2$ 是由 $I$，$J$ 和 $A$ 生成的代数. 因此 $G$ 是强正则的.

**问题 31I** 设图 $G$ 是一个 $srg(v, k, \lambda, \mu)$. $\Delta(x)$的特征值与 $G$ 的特征值

$$k, r, r, \cdots, r, s, s, \cdots, s \quad (\text{比如说 } r > s)$$

交错. 与此交错的任何一个序列可以至多有一项大于 $r$.

半-情形除外，$r$ 和 $s$ 是满足 $rs=\mu-k$ 的整数；特别地，$r\leqslant k-\mu$(即使在半-情形). 图 $\Delta(x)$是 $k-\mu$ 度的正则图. 当图不连通时，$k-\mu$ 是$\Delta(x)$的重数大于 1 的一个特征值. [571]

**问题 31J** 对应于特征值 1 的特征空间 $A$ 和对应于$-1$ 的特征空间 $B$ 的维数都是 5，且包含在与全幺向量正交的 9 维的向量空间中，因此在这两个特征空间的交中存在一个非零向量 $\boldsymbol{u}$. 证明 $K$ 的连通性导致与定理 31.11 矛盾.

**问题 31K** (i)由定理 31.13 或其证明的部分得出. (ii)(31.6)乘以 $J$. (iii)无向边的数目是 $A^2$ 的迹的一半. (iv)证明这些无向边没有一个公共的顶点而且它们不被一条边连结. 到反转方向时，只剩下一种方式完成这个图.

**问题 32A** 这些图中的一个有两个顶点，一个有三个顶点，两个有四个顶点.

**问题 32B** (i)设 $X$ 是从 $s$ 由一条有向路可达到的顶点的集合，在这条路的所有边上 $f(e)>0$. 又设 $Y$ 为余下的顶点，如果有的话. 如果 $t\notin X$，得到与等式(7.1)的矛盾. (为什么?)(ii)对 $k$ 用归纳法.

**问题 32C** 赋予 $D$ 的所有边容量 1. 利用定理 7.1.

**问题 32D** 如果$(H, K)$是一个 $\ell$-分离且删去 $\ell$ 个顶点 $S:=V(H)\cap V(K)$不使该图不连通，则 $H$ 和 $K$ 中至少有一个的顶点集包含在 $S$ 中.

**问题 33A** 简要解释为何 $G$ 的包含边 $e$ 的生成树与 $G''_e$ 的生成树一一对应，而且为何 $G$ 的不包含边 $e$ 的生成树与 $G'_e$ 的生成树一一对应.

**问题 33B** 寻找形式为 $f(\lambda)+(-1)^n g(\lambda)$的答案. 利用归纳法、等式(32.1)和例 32.1.

**问题 33C** 更强一些，$K_{3,3}$(这里边由路代替)的一个剖分图作为彼得森图的一个子图出现. [572]

**问题 33D** 假设 $G''_S$ 的一个顶点与三条不同的边 $e_1$，$e_2$ 和 $e_3$ 关联. 这样的顶点是$G:S$的一个连通分支 $C$. 因此 $e_i$ 有一个端点 $x_i$ 在 $C$ 中，$i=1, 2, 3$(这些端点不必各不相同). 解释为何 $C$ 的连通性蕴涵存在一个顶点 $x$ 和 $C$ 中从 $x$ 到 $x_1$，$x_2$ 和 $x_3$ 的可能退化但内部不相交的路. 也就是说，我们有 $C$ 的一个子图与字母 $Y$ 的剖分图同构，但每个 $x_i$ 在 $Y$ 的臂的端点且路径的长度都$\geqslant 1$，否则，某些臂可能是退化的. 由这个观察立刻导出该问题第一部分的解.

给定一个连通图 $C$ 的四个顶点 $x_i$，$i=1, 2, 3, 4$，证明存在一个子图或者同构于字母 $X$ 的剖分图，或者同构于字母 $I$ 的剖分图，但可能有退化的臂且 $x_i$ 在臂的端点.

如果 $K_5$ 的一个顶点，比如说 1，用两个由一条边相连的顶点 $1_L$ 和 $1_R$ 代替，且 1 连结其他顶点的边并分开，比如说 $1_L$ 连结 2 和 3，$1_R$ 连结 4 和 5，则检验得到的图有 $K_{3,3}$作为一个子图. 把这个结果与前面的观察结合起来完成这个问题.

**问题 33E** 利用欧拉公式. 除了与五个柏拉图立体对应的(3，3)，(3，4)，(3，5)，(4，3)，(5，3)之外出现的仅有的对子$(d_1, d_2)$是$(2, n)$和$(n, 2)$，$n\geqslant 2$，它们与多边形和键图对应.

**问题 34A** 我们有从顶点集 $V(G)$ 的所有子集 $X$ 的 $\mathbb{F}_2$ 上的向量空间到 $G$ 的割集空间的一个线性映射，即 $X \mapsto \times(X, V(G)\setminus X)$.（这个映射的矩阵是关联矩阵 $N$.）在这个映射的核中，集合 $X$ 是什么？割集空间的维数等于图的顶点数减去核的维数.

**问题 34B** 对码字的支持的基数用归纳法.

[573] **问题 34C** $G'_e$ 的回路恰是 $G$ 中不包含 $e$ 的那些回路. $H''_e$ 的键是什么？

**问题 34D** 做这个问题的一个途径是，关于连通图 $K$ 的边集的一个子集 $S$，首先证明两件事：(1)$S$ 是 $K$ 中一棵生成树的边集，当且仅当 $K$ 中没有回路被 $S$ 包含且 $S$ 相对于这个性质是最大的，(2)$S$ 是 $K$ 中一棵生成树的边集，当且仅当 $K$ 的每个键与 $S$ 非平凡地相交且 $S$ 相对于这个性质是最小的.

**问题 34E** 首先证明从一个连通的三价图中删去一条割边得到的两个分支有奇数个顶点.

**问题 34F** 这里是构造键的一个想法. 删去 $G$ 的一棵生成树的任意一条边留下有两个分支的一个子图，端点各在一个分支中的边的集合是 $G$ 的一个键.

**问题 34G** 从一个连通图 $G$ 中删去一个键 $S$ 的边总给出有两个分支的图，回忆定义 $G'_S$ 时选择删去孤立的顶点. 在(ii)中，码的等价性给出 $H$ 和 $G$ 的边集之间的一个一一对应，它把回路映到回路，键映到键. 利用(i)及没有孤立顶点的图是不可分的当且仅当任意两条边一起被包含在一个环路中这一事实，参见定理 32.2.

**问题 34H** 在 $G$ 中给定一个多边形 $P$，可以考虑子图 $H$ 和 $K$，这里 $H=P$ 且 $K$ 是包含不在 $P$ 中的 $G$ 的所有边的 $G$ 的一个生成子图.

考虑 $G$ 中的一个键 $B$，$B$ 由一端在 $X$ 中且另一端在 $Y$ 中的所有边组成，这里 $X$ 和 $Y$ 是 $V(G)$ 的划分且每个导出一个连通子图. 假设与 $G$ 是塔特-$k$-连通的矛盾，但 $|B|=\ell<k$. 设 $\ell_1$ 是与 $B$ 中的边关联的 $X$ 中的顶点的数目. 如果由 $X$ 导出的子图至少有 $\ell_1$ 条边，则容易找到 $G$ 的一个 $\ell_1$-分离. 处理余下的情形.

**问题 34I** 我们给出独立的提示，尽管能从(ii)导出(i)，或如我们提到过的，前两部分能
[574] 从(iii)导出.

(i)如果 $A$ 和 $B$ 是多边形 $P$ 和 $Q$ 的边集，从边 $y$ 开始沿两个方向经过 $P$，一旦到达 $Q$ 的顶点就停止.

(ii)如果 $A$ 和 $B$ 是码字 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的支撑，$\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的某个线性组合的支撑 $S$ 包含坐标 $y$ 但不包含 $x$. 通过对 $|S|$ 用归纳法，证明一个码字的任何一个支撑 $S$ 是码字的最小支撑的并.

(iii)证明：一般地，如果 $z\in\overline{S}$，则存在一个极小相关集 $D$ 使得 $z\in D\subseteq S\cup\{z\}$（复习引理 23.2). 然后证明 $y$ 在 $(A\cup B)\setminus(x, y)$ 的闭包中.

**问题 35A** 取 $K_n$ 的顶点为 $\mathbb{Z}_n$. 对 $n=5$，使用 $[1, 2, 4, 3] \pmod 5$ 的所有循环移位(平移).

**问题 35B** 在例 21.4 的描述中去掉最后一个坐标，并把克莱布什图描述为有顶点集 $\mathbb{F}_2^4$ 且当 $\boldsymbol{x}+\boldsymbol{y}$ 的重量为 3 或 4 时，$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 相邻. 试着选择一条步路 $w$，其他路径通过 $w$ 被 $\mathbb{F}_2^4$ 的所有元素平移而得到.

**问题 35C** (i)类似于定理 33.5. 至于网的唯一性的证明，可以取 $V(K_7)=$

{0, 1, …, 6}，不失一般性，经过 0 的步路是

$$[6,0,1],[1,0,2],[2,0,3],[3,0,4],[4,0,5],[5,0,6].$$

经过边(6, 1)的步路有第三个顶点 3 或 4(否则顶点条件在 1 或 6 被违反)，在任一种情形其他步路是唯一确定的.

**问题 35D** 图 $\mathcal{M}_x$ 的顶点是与 $x$ 关联的边. 这些边来自 $G$ 中一个键的边集，因此是 $H$ 中一个回路的边.

**问题 35E** 用术语旗标表示由一个顶点 $x$、与 $x$ 关联的一条边 $e$ 以及与 $e$ 关联的一个面 $F$ 构成的三元组($x$, $e$, $F$). 恰好存在另一个顶点 $x'$ 使得($x'$, $e$, $F$)是旗标，恰好另一条边 $e'$ 使得($x$, $e'$, $F$)是旗标，且恰好另一个面 $F'$ 使得($x$, $e$, $F'$)是旗标；因此这些对象在固定($x$, $e$, $F$)的项的任意一个自同构下保持不动.

575

**问题 35F** 利用定理 35.1. $K_{n,n}$ 能嵌入在一个可定向的曲面上使得所有的面是四边形的最小的 $n(n>2)$ 值是 $n=6$；$n$ 一定是偶数，但 $K_{4,4}$ 在 $\mathcal{T}_0$ 中没有这样的嵌入. 需要对情形的一些思路和/或分析.

**问题 35G** 所有的面有相同的规模. 考虑过边(0, 1)的步路. 接下来的几条边是(1, $1-\omega$)，($1-\omega$, $1-\omega+\omega^2$)，($1-\omega+\omega^2$, $1-\omega+\omega^2-\omega^3$)，等等. 例如，如果 $m\equiv 2 \pmod 4$，则该步路有长度 $m/2$.

**问题 36A** $M$ 的所有$(n-1)\times(n-1)$主子矩阵的行列式之和等于一个适当的符号乘以 $M$ 的特征多项式 $\det(xI-M)$中 $x$ 的系数.

**问题 36B** 存在这样一棵树形图，对每个映射 $f$：{2, 3, …, $n$}→{1, 2, …, $n-1$}使得对每个 $i$，$f(i)<i$.

**问题 36C** 如果坐标由 $E(H)$指示的一个向量 $g$ 有以下性质：对每条闭步路 $w$，$g$ 在 $w$ 的边上的值带符号的和等于零，则定义由 $V(H)$指示的一个向量 $h$ 如下.（为了方便，假设 $H$ 是连通的，否则要单独处理每个分支.）固定一个顶点 $x$，定义 $h(x):=0$，且对每个顶点 $y$，设 $h(y)$是 $g$ 在从 $x$ 到 $y$ 的任意一条步路的边上的值带符号的和. 检验 $h$ 是定义好的且 $g$ 是 $h$ 的上边缘.

**问题 36D** 设$\mathcal{Z}$表示圈空间且$\mathcal{B}$表示上边缘空间，这些空间是正交互补的，因此它们的(直)和是$\mathbb{R}^m$(其坐标由 $E(D)$指示的所有向量的空间). 证明线性变换 $R$ 在$\mathcal{Z}$上是一一的且$\mathcal{Z}R\cap\mathcal{B}=\{0\}$,所以$\mathbb{R}^m$是这些子空间的直和.

**问题 36E** 在图 36.4 中，所有正方形的边长可以用三个被指示的正方形的边长 $x$，$y$ 和 $z$ 的整数线性组合表示. 例如，最小的正方形的边长为 $z-x$，次小的正方形的边长为 $x+z-y$. 可以发现有些正方形的大小能用多种方式表示，因此我们有 $x$，$y$，$z$ 之间的线性关系. 最终，可以把任何一个正方形的边长表示为 $x$ 的一个有理数倍，这些有理数的最小公分母是应取的 $x$ 值.

576

**问题 36F** 最快的可能是像问题 36E 那样进行，例如，设 $x$，$y$，$z$ 表示三条边上的电流，等等. 但可以计算如等式(36.3)中的行列式得到问题的解.

**问题 37A** 旋转包括：单位元(1)，围绕穿过两个对面的中心的轴转动 90 度、180 度和

270 度(3+3+3)，围绕穿过两个对边的中心的轴转动 180 度(6)，以及围绕穿过两个相对顶点的轴转动 120 度和 240 度(2+2+2+2). 例如，后面的 8 个转动对圈指标提供了 $8X_3^2$.

**问题 37B** 利用定理 37.2 和问题 37A.

**问题 37C** 解释为何由($\sigma$, $\tau$)固定的单射 $f$ 的数目仅仅与 $\sigma$ 和 $\tau$ 的圈结构有关(即对每个 $i$，依赖长度为 $i$ 的圈的数目 $z_i$)，并寻找用 $z_i(\sigma)$和 $z_i(\tau)$表示单射数目的表达式.

**问题 37D** 在定理 37.3 中，取 $G$ 是二面体群且 $H$ 为对称群 $S_2$.

**问题 37E** 如果立方体的一个旋转 $\rho$ 在面上有 $a$ 个圈且在顶点上有 $b$ 个圈，则由 $\rho$ 固定的染色的数目是 $t^a s^b$. 利用伯恩赛德引理.

**问题 38A** 设 $m :=v/2$. 对 $M :=v-1$ 种颜色中的每一种 $i$，通过取染颜色 $i$ 的边、与染颜色 $i$ 的边不关联的所有顶点 $x$ 的单元素集$\{x\}$，以及为构造一个 $m$-划分所需的足够多的空集，得到 $V(K_v)$的一个 $m$-划分. 检验条件(38.1)成立. 复习定理 38.1 的证明.

577

# 附录 2 形式幂级数

在介绍本附录的主题之前，首先说明这里给出的许多断言没有给予证明. 在这种情况下，作出证明对读者而言是容易的练习.

考虑集合

$$\mathbb{C}^{\mathbb{N}_0} := \{(a_0, a_1, a_2, \cdots) : \forall_{i\in\mathbb{N}_0}[a_i \in \mathbb{C}]\}.$$

在这一集合上引入加法运算和乘法运算如下：

$$(a_0, a_1, \cdots) + (b_0, b_1, \cdots) := (a_0 + b_0, a_1 + b_1, \cdots),$$

$$(a_0, a_1, \cdots)(b_0, b_1, \cdots) := (c_0, c_1, \cdots),$$

这里 $c_n := \sum_{i=0}^{n} a_i b_{n-i}$.

这个定义产生一个环，记该环为$\mathbb{C}[[z]]$并称之为*形式幂级数环*. 这个名称按如下的方式加以解释. 设 $z := (0, 1, 0, 0, \cdots)$. 则 $z^n$ 是序列$(0, \cdots, 0, 1, 0, \cdots)$，这里 1 在第 $n$ 个位置. 于是，形式上我们有

$$\boldsymbol{a} = (a_0, a_1, \cdots) = \sum_{n=0}^{\infty} a_n z^n =: a(z).$$

我们使用两种记法，即 $\boldsymbol{a}$ 和 $a(z)$来表示该序列. 我们说 $a_n$ 是 $\boldsymbol{a}$(或 $a(z)$)中 $z^n$ 的*系数*. 注意，系数在$\mathbb{C}$中的多项式环$\mathbb{C}[z]$是$\mathbb{C}[[z]]$的子环. 一些幂级数在分析学的意义上收敛. 对这些级数，可以利用分析学中的结果. 这些结果往往可以从形式的意义上证明，亦即不利用分析中的收敛或其他工具加以证明.

578

**例 1** 设 $f := (1, 1, 1, \cdots)$. 利用乘法的定义以及 $1 - z = (1, -1, 0, \cdots)$，可以发现 $(1-z)f = (1, 0, 0, \cdots) = 1$. 于是，在$\mathbb{C}[[z]]$中，我们有 $f = (1-z)^{-1}$，亦即

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n,$$

这是分析学中已知的结果.

$\mathbb{C}[[z]]$ 中的正则元素是 $a_0 \neq 0$ 的幂级数. 这由乘法的定义可以立刻看出. 从关系 $a(z)b(z) = 1$ 可以计算系数 $b_n$，因为 $b_0 = a_0^{-1}$ 且 $b_n = -a_0^{-1}\sum_{i=1}^{n} a_i b_{n-i}$. 由此可知$\mathbb{C}[[z]]$的商域与所谓的*洛朗*(Laurent)*级数* $\sum_{n=k}^{\infty} a_n z^n$ 等同，这里 $k \in \mathbb{Z}$. 因为它今后起着进一步的作用，我们给 $z^{-1}$ 的系数一个分析学中熟知的名字. 如果 $a(z)$ 为级数，我们说 $a_{-1}$ 是 $a(z)$ 的*留数*. 并写成 $\operatorname{Res} a(z)$.

设 $f_n(z) = \sum_{i=0}^{\infty} c_{ni} z^i (n = 0, 1, 2, \cdots)$ 是$\mathbb{C}[[z]]$的元素，它具有性质

$$\forall_i \exists_{n_i} [n > n_i \Rightarrow c_{ni} = 0].$$

则可以形式地定义

$$\sum_{n=0}^{\infty} f_n(z) = \sum_{i=0}^{\infty} \Big( \sum_{n=0}^{n_i} c_{ni} \Big) z^i. \tag{1}$$

这一定义允许我们对幂级数 $a(z)$ 的"变量" $z$ 引入幂级数 $b(z)$ 的代换. 如果 $b_0=0$，还写成 $b(0)=0$，则幂 $b^n(z):=(b(z))^n$ 满足形式加法的条件，即

$$a(b(z)):=\sum_{n=0}^{\infty}a_n b^n(z)$$

579 有意义.

**例 2** 设 $f(z):=(1-z)^{-1}$，$g(z)=2z-z^2$. 则形式上

$$h(z):=f(g(z))=1+(2z-z^2)+(2z-z^2)^2+\cdots$$
$$=1+2z+3z^2+4z^3+\cdots.$$

从微积分学我们知道这是 $(1-z)^{-2}$ 的幂级数展开，因此这个结果在 $\mathbb{C}[[z]]$ 中肯定正确. 事实上，我们有

$$(1-z)h(z)=\sum_{n=0}^{\infty}z^n=(1-z)^{-1}.$$

这个结果来自(合法的)代数运算：

$$f(g(z))=(1-(2z-z^2))^{-1}=(1-z)^{-2}.$$

我们常常用幂级数表示常用的函数，并在很多情况下反函数也用幂级数表示. 这可由 $f_0=0$ 且 $f_1\neq 0$ 的级数 $f(z)$ 形式地加以解释. 由代换"解"方程 $f(g(z))=z$. 这给出 $f_1g_1=1$，$f_1g_2+g_1^2=0$，并且一般地，$z^n$ 的系数的表示以 $f_1g_n$ 开始，其他的项仅涉及系数 $f_i$ 和 $k<n$ 的系数 $g_k$. 把这个表示置为 0 可以求出 $g_n$.

**例 3** 喜欢组合学挑战的读者可以给出计数公式

$$\sum_{k=0}^{n}\binom{2k}{k}\binom{2n-2k}{n-k}=4^n$$

的一个证明. 这等价于证明形式幂级数 $f(z):=\sum_{n=0}^{\infty}\binom{2n}{n}(z/4)^n$ 满足关系式 $f^2(z)=(1-z)^{-1}$. 由类似的论证或通过代数运算可以找到名为 $(1+z)^{\frac{1}{2}}$ 的形式幂级数.

现在我们考虑形式幂级数 $f(z):=2z+z^2$. 上面描述过的"反函数"过程产生满足 $2g(z)+$
580 $g^2(z)=z$ (亦即 $(1+g(z))^2=1+z$) 的幂级数 $g(z)$. 于是，这应是称之为 $(1+z)^{\frac{1}{2}}$ 的幂级数. 对收敛幂级数成立的代数关系在形式幂级数理论中为真就不再令人惊奇了.

**注记** 我们指出，在微积分学中完全有意义的代换在目前的理论中可能遭到禁止. 幂级数 $\sum_{n=0}^{\infty}\frac{z^n}{n!}$ 当然被命名为 $\exp(z)$. 在微积分学中，可以用代换 $z=1+x$ 并找出 $\exp(1+x)$ 的幂级数. 在形式加法之下这是不允许的.

下面引入幂级数的形式导数.

**定义** 如果 $f(z)\in\mathbb{C}[[z]]$，则定义导数

$$(Df)(z)=f'(z)$$

为幂级数 $\sum_{n=1}^{\infty}nf_nz^{n-1}$.

读者利用本附录中的定义证明如下的法则应该没有什么困难：

(D1)$(f(z)+g(z))'=f'(z)+g'(z)$.

(D2)$(f(z)g(z))'=f'(z)g(z)+f(z)g'(z)$.

(D3)$(f^k(z))'=kf^{k-1}(z)f'(z)$.

(D4)$(f(g(z)))'=f'(g(z))g'(z)$.

链式法则(D4)是一个更一般的断言，即

$$D\Big(\sum_{n=0}^{\infty}f_n(z)\Big)=\sum_{n=0}^{\infty}D(f_n(z))$$

的特例.

如果收敛起作用，则这是一个带附加条件的较难的定理，但对形式幂级数该定理是平凡的！

熟知的商的求导法则也容易被证明. 于是可以把该理论推到洛朗级数. 我们需要以下两条事实，它们的证明再次留给读者作为练习.

如果 $w(z)$ 为洛朗级数，则

(R1)$\mathrm{Res}(w'(z))=0$.

(R2)$w'(z)/w(z)$的留数是使得 $w(z)$ 中的系数 $z^{\ell}$ 不为零的最小整数 $\ell$. 581

我们已经提到"反函数"的概念，并且已经表明如何递归地计算其系数. 下面的定理给出系数的一个表示.

**定理 1** 设 $W(z)=w_1z+w_2z^2+\cdots$ 是一个 $w_1\neq0$ 的幂级数. 又设 $Z(w)=c_1w+c_2w^2+\cdots$ 是 $w$ 的幂级数，使得 $Z(W(z))=z$. 则

$$c_n=\mathrm{Res}\Big(\frac{1}{nW^n(z)}\Big).$$

**证明** 观察到 $c_1=w_1^{-1}$. 现在我们把形式导数用于关系式 $Z(W(z))=z$. 这得出

$$1=\sum_{k=1}^{\infty}kc_kW^{k-1}(z)W'(z). \tag{2}$$

考虑(2)的右边除以 $nW^n(z)$ 得到的级数. 如果 $n\neq k$，则由(D3)项 $W^{k-1-n}(z)W'(z)$ 是导数且因此由(R1)其留数为 0. 利用(R2)于 $n=k$ 的项可以得到定理的断言. ■

这个定理使我们有可能只利用形式幂级数理论给出拉格朗日反演公式(参见定理 14.3)的一个证明. 设 $f(z)$ 为 $f_0\neq0$ 的幂级数，则 $W(z):=z/f(z)$ 是 $w_1\neq0$ 的幂级数. 现在我们应用定理 1. 可以发现

$$c_n=\mathrm{Res}\Big(\frac{f^n(z)}{nz^n}\Big)=\frac{1}{n!}(D^{n-1}f^n)(0)$$

的 $z=\sum_{n=1}^{\infty}c_nw^n$，如(14.19)所确定的. 这一方法基于 P. Henrici, An algebraic proof of the Lagrange-Bürmann formula, *J. Math. Anal. and Appl.* 8(1964), 218-224. 优美的简化属于 J. W. Nienhuys.

正如上面观察到的，我们定义

$$\exp(z):=\sum_{n=0}^{\infty}\frac{z^n}{n!}. \tag{3}$$

582

从上面的知识我们期望用 $-z$ 代替 $z$ 会在环$\mathbb{C}[[z]]$中产生逆元素. 形式乘法以及对 $n>0$ 有 $\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$ 的事实证明这是正确的.

现在，可以定义

$$\log(1+z):=\sum_{n=1}^{\infty}(-1)^n\frac{z^n}{n}. \tag{4}$$

微积分学使我们再次期望“函数”log 和 exp 之间的关系. 由代换法则，考虑幂级数 $\log(\exp(z))$ 是有意义的. 由(D4)可以发现

$$D(\log(\exp(z)))=\frac{\exp(z)}{\exp(z)}=1,$$

即 $\log(\exp(z))=z$. (这里利用了 $\log(1+z)$的形式导数是$(1+z)^{-1}$这一事实.)

当然，还有很多关于形式幂级数的知识. 可以探索分析学中有多少熟悉的结果可以推到形式幂级数上，或者给出形式的证明. 我们希望这一简单的讨论已足以启发读者. 583

# 人名索引

索引中的页码为英文原书页码，与书中页边标注的页码一致．

# 主题索引

索引中的页码为英文原书页码，与书中页边标注的页码一致．



⊖ 这里，ff 是指该页及其后．——编辑注

## C

## D

**E**

## F



## G

H



I

## J



## K



## L

## M



## N

## O



## P

## Q

## R



## S

**T**

## U



## V



## W



## Y



## Z